

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Masato YAMAMICHI et al. :
Serial No. NEW : **Attn: APPLICATION BRANCH**
Filed October 8, 2003 : Attorney Docket No. 2003_1411A
ENCIPHERMENT APPARATUS, DECRYPTON THE COMMISSIONER IS AUTHORIZED
APPARATUS AND ENCRYPTON SYSTEM TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450


Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-296219, filed October 9, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masato YAMAMICHI et al.

By 
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
October 8, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年10月 9日

出 願 番 号
Application Number:

特願2002-296219

[ST.10/C]:

[JP2002-296219]

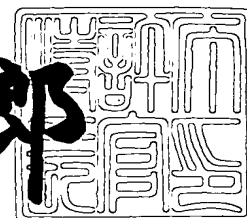
出 願 人
Applicant(s):

松下電器産業株式会社

2003年 6月 5日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3043722

【書類名】 特許願

【整理番号】 2022540381

【提出日】 平成14年10月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 5/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
社内

 【氏名】 山道 将人

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
社内

 【氏名】 布田 裕一

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
社内

 【氏名】 大森 基司

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
社内

 【氏名】 館林 誠

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100097445

 【弁理士】

 【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 暗号システム、送信装置及び受信装置

【特許請求の範囲】

【請求項 1】 外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置であって、

前記受信装置毎に乱数パラメータを記憶する記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする、送信装置。

【請求項 2】 前記暗号手段は、NTRU暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする、請求項 1 に記載の送信装置。

【請求項 3】 前記制御手段は、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項 1 または請求項 2 に記載の送信装置。

【請求項 4】 前記制御手段は、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項 1 または請求項 2 に記載の送信装置。

【請求項 5】 外部から暗号文を受信し、復号鍵で復号する受信装置であって、前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段と、

前記復号文が正しく得られたかどうかを判別する判別手段と、

前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする、受信装置。

【請求項 6】 外部から入力された平文を暗号化した暗号文を送信する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、

前記送信装置は、

乱数パラメータを記憶するパラメータ記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記暗号文を送信する送信手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、

前記受信装置は、

前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする、暗号システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、同じ復号鍵を使用し続けると暗号化通信が徐々に復号できなくなっていく暗号システムに関するものである。

【 0 0 0 2 】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献 1 参照。）。

【 0 0 0 3 】

この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータを上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信データを受信する。そして、受信装置は、暗号化された通信データを、自身の有する秘密鍵で復号して元の通信データを得る。

【 0 0 0 4 】

ここで、もしも通信先受信装置の有する秘密鍵が暴露されると、上記の暗号システムは、もはや安全ではなくなる。通信先受信装置の公開鍵で暗号化された通信内容は、暴露された秘密鍵をもつ第三者の受信装置でも復号されてしまうからである。従って、受信装置の有する秘密鍵は、外部に露見しないように厳重に管理する必要がある。

【 0 0 0 5 】

しかしながら、場合によっては、何らかの事故や事件により受信装置の有する秘密鍵が暴露されてしまう可能性がある。従って、上記の暗号システムにおいては、受信装置の有する秘密鍵が暴露された場合、もしくはその疑いがある場合には、暴露された秘密鍵と対になる公開鍵の使用を停止する必要がある。

【 0 0 0 6 】

そのような方法の例として、証明書廃棄リスト (Certificate Revocation List、CRL) と呼ばれるデータ構造を使用して、受信装置の有する秘密鍵が暴露された場合に、暴露された秘密鍵と対になる公開鍵の使用を停止する方法が開示されている (例えば、非特許文献 2 参照。)。

【 0 0 0 7 】

また、他の例として、IEEE (Institute of Electrical and Electronics Engineers) 1394 規格によるシリアルバス上を伝送されるデジタルコンテンツを保護する DTCP (Digital Transmission Content Protection) 規格の中では、SRM (System Renewability Messages) を使用して、受信装置の有する秘密鍵が暴露された場合に、当該受信装置の公開鍵の使用を停止するようになっている (例えば、非特許文献 3 参照。)。

【 0 0 0 8 】

以下に、これらの方法を簡単に説明する。

【 0 0 0 9 】

まず、公開鍵は、それを保有する人や物などの識別情報に関連付けられ、信頼

できる第三者機関によりシリアル番号等が付加された形式に変換される。さらに他者による改ざんを防止するためにその第三者機関のデジタル署名を付加する。これを公開鍵証明書と呼ぶ。そして、第三者機関により発行されるCRLやSRMには、秘密鍵の暴露等の理由で使用を停止すべき公開鍵証明書のシリアル番号が記載されている。よって、CRLやSRMに記載されたシリアル番号をチェックすることにより、暴露された秘密鍵と対になる公開鍵の使用を停止することができる。

【0010】

この方法を、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵証明書のデジタル署名を確認し、その公開鍵証明書から、公開鍵とシリアル番号を取得し、第三者機関から発行されるCRLやSRMを取得する。そして、送信装置は、取得した公開鍵証明書のシリアル番号がCRLやSRMに記載されていれば、その公開鍵の使用を停止する。このことにより、受信装置の有する秘密鍵が暴露されている場合、暴露された秘密鍵と対になる公開鍵の使用を停止することができる。よって、これにより、送信装置と受信装置の間で安全な暗号化通信を実現することができる。

【0011】

【非特許文献1】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997

【非特許文献2】

山田信一郎 訳、「デジタル署名と暗号技術」、株式会社ピアソン・エデュケーション、p. 159～p. 214、1997

【非特許文献3】

D i g i t a l T r a n s m i s s i o n C o n t e n t P r o t e c t i o n S p e c i f i c a t i o n R e v i s i o n 1. 2 (I n f o r m a t i o n a l V e r s i o n) 、 [o n l i n e] 、 2 0 0 1 年 7 月 1 1 日 、 [2 0 0 2 年 9 月 1 3 日 検 索] 、 インターネット<URL: http://www.dtcp.com/data/info_dtcp_v1_1

2_20010711.pdf>

【0012】

【発明が解決しようとする課題】

しかし、CRLやSRMを用いた上記方法では、以下のような課題がある。

【0013】

(1) 送信装置が最新のCRLやSRMを取得できない場合、受信装置の有する秘密鍵が暴露されていても、送信装置は必ずしも当該受信装置の公開鍵の使用を停止できない。これにより、従来の技術では、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

【0014】

(2) 暗号化通信の安全性確保のためには、鍵を定期的に更新することが望ましい。しかし、従来の技術では、鍵を定期的に更新しなくても受信装置は正常に動作するため、受信装置を扱う人に、鍵の更新を促しにくい。

【0015】

(3) 信頼できる第三者機関によるCRLやSRMが必要である。

【0016】

以下に、上記問題点(1)、(2)、(3)について詳細を説明する。

【0017】

まず、CRLやSRMを用いた上記方法では、送信装置が最新のCRLやSRMを取得できず、受信装置の有する秘密鍵が暴露されていても、当該受信装置の公開鍵の使用を停止できない場合がある。例えば、デジタル化された映画コンテンツデータがDVDなどの記録媒体に記録されるシステムであって、映画コンテンツデータは受信装置に相当するプレーヤ毎の暗号鍵で暗号化されてディスクに記録され、プレーヤはこの暗号鍵に対応する復号鍵を有しており、ディスクに記録されている暗号化映画コンテンツデータを復号して、映画を再生するものであり、さらに特定のプレーヤは不正な機器であって再生を防止する目的で、そのプレーヤの公開鍵のCRLやSRMがDVD等の記憶媒体に記録されて発行されるような場合である。

【 0 0 1 8 】

いま、ある受信装置の秘密鍵が暴露したことが判明したとする。それ以降は、当該受信装置の公開鍵証明書シリアル番号が追加記載された最新のCRLやSRMは、DVDに記録されて発行されるが、それ以前に配布されたDVDには古いCRLやSRMが記録されたままである。結果として、古いDVDを用いていると、古いCRLやSRMしか取得できず、必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。

【 0 0 1 9 】

また、SRMを用いるDTCP規格では、IEEE1394シリアルバスで接続された機器間で、機器が持つ古いSRMは他の機器が持つ新しいSRMに更新されていく。すなわち、この仕組みによって、DVD等の記憶媒体から新しいSRMを取得する以外にも、他の機器からも新しいSRMを取得できる。しかしながら、この仕組みを用いても、完全には最新のSRMを取得できる保証は無い。結果として、送信装置は必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。従って、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

【 0 0 2 0 】

次に、CRLやSRMを用いた上記方法では、受信装置を扱う人に、自身の公開鍵・秘密鍵の更新を促しにくい。これは、送信装置が、CRLやSRMにより受信装置の公開鍵の使用を停止するまでは、受信装置は、完全に暗号化通信を復号し続けることが可能であることに起因する。以下にこのことを説明する。

【 0 0 2 1 】

従来の技術では、暴露された秘密鍵と対になる公開鍵の使用を停止するためには、最新のCRLやSRMを第三者機関のサーバ等から取得して、CRLやSRMに記載されたシリアル番号をチェックしなければならない。しかし、一般に、送信装置を扱う人は、CRLやSRMのチェックを知らずに暗号化通信を行ったり、あるいはサーバ等から最新のCRLやSRMを取得するのが面倒なために、このチェックを無視して暗号化通信を行ったりすることが多い。これは、送信装置が受信装置の公開鍵を取得していれば、CRLやSRMのチェックを行わなく

とも、送信装置、受信装置共に正常に動作して、暗号化通信を行うことができるからである。そして、送信装置がCRLやSRMのチェックを行わないで暗号化通信を行うと、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を更新しようとはしない。なお、公開鍵証明書に有効期限を設け、送信装置が有効期限の切れた公開鍵の使用を停止し、受信装置が鍵を更新しない限り、送信装置から受信装置への暗号化通信を行わないようにする方法もある。しかしながら、この場合も、CRLやSRMを用いる方法と同様に、送信装置を扱う人は有効期限のチェックを知らずに、あるいはこのチェックを無視して暗号化通信を行うことが多い。この結果、CRLやSRMを用いる方法と同様に、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を定期的に更新しようとはしない。

【0022】

最後に、CRLやSRMを用いた上記方法では、信頼できる第三者機関によるCRLやSRMが前提となっている。これは、信頼できる第三者機関によるCRLやSRMの存在を仮定しなければならない点が問題点である。

【0023】

そこで、本発明は上記（１）、（２）、（３）の課題に鑑み、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第１の目的とする。

【0024】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、同じ秘密鍵を使い続けると、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることを第２の目的とする。

【0025】

また、送信装置が暗号化通信を行うに際して、第三者機関によるCRLやSRMを必要としない暗号システム、送信装置又は受信装置を提供することを第3の目的とする。

【0026】

【課題を解決するための手段】

請求項1における発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

【0027】

請求項2における発明は、請求項1に記載の送信装置が、NTRU暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする。

【0028】

請求項3における発明は、請求項1または請求項2に記載の送信装置において、前記制御手段が、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

【0029】

請求項4における発明は、請求項1または請求項2に記載の送信装置において、前記制御手段が、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

【0030】

請求項5における発明は、外部から暗号文を受信し、復号鍵で復号する受信装置が、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段と、前記復号文が正しく得られたかどうかを判別する判別手段と、前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする。

【0031】

請求項6における発明は、外部から入力された平文を暗号化した暗号文を送信

する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、前記送信装置は、乱数パラメータを記憶するパラメータ記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記暗号文を送信する送信手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、前記受信装置は、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【 0 0 3 2 】

【発明の実施の形態】

以下、本発明に係る暗号システムの実施の形態について、図面を用いて説明する。

【 0 0 3 3 】

本発明に係る暗号システムは、公開鍵暗号方式の一例として、NTRU暗号方式を用いる。NTRU暗号方式は、多項式の演算で暗号化と復号化を行う公開鍵暗号方式である。このNTRU暗号方式、及びNTRU暗号方式の公開鍵、及び秘密鍵の生成方法については、Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, 「NTRU: A ring based public key cryptosystem」, Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998. に詳しく述べられているので、ここでは詳細な説明を省略するが、以下にNTRU暗号方式について簡単に説明する。

【 0 0 3 4 】

NTRU暗号方式は、整数のシステムパラメータ、 N 、 p 、 q を持つ。上記文献には、システムパラメータの例として、 $(N, p, q) = (107, 3, 64)$ 、 $(N, p, q) = (167, 3, 128)$ 、 $(N, p, q) = (503, 3, 256)$ の3つの例が挙げられている。

【 0 0 3 5 】

以降、本発明に係る暗号システムの実施の形態では、システムパラメータ N を

N = 1 6 7 とした場合の説明を行う。

【 0 0 3 6 】

N T R U 暗号方式は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。まず、N T R U 暗号方式で扱う多項式は、上記システムパラメータ N に対し、N - 1 次元以下の多項式であり、例えば N = 5 のとき、 $X^4 + X^3 + 1$ 等の多項式である。ここで、「 X^a 」は X の a 乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵 h、秘密鍵 f、平文 m、乱数 r、暗号文 c はいずれも、N - 1 次元以下の多項式として表現される（以降、それぞれを公開鍵多項式 h、秘密鍵多項式 f、平文多項式 m、乱数多項式 r、暗号文多項式 c と呼ぶ）。

【 0 0 3 7 】

そして、多項式演算は、上記システムパラメータ N に対し、 $X^N = 1$ という関係式を用いて、演算結果が常に N - 1 次元以下の多項式になるように演算される。例えば、N = 5 の場合、多項式 $X^4 + X^2 + 1$ と多項式 $X^3 + X$ の積は、多項式と多項式の積を \times 、整数と多項式の積を \cdot とすると、 $X^5 = 1$ という関係から、

$$\begin{aligned} & (X^4 + X^2 + 1) \times (X^3 + X) \\ &= X^7 + 2 \cdot X^5 + 2 \cdot X^3 + X \\ &= X^2 \times 1 + 2 \cdot 1 + 2 \cdot X^3 + X \\ &= 2 \cdot X^3 + X^2 + X + 2 \end{aligned}$$

というように、常に N - 1 次元以下の多項式になるように演算される。

【 0 0 3 8 】

暗号化時には、以下に述べる乱数多項式 r と公開鍵多項式 h とを用いて、平文多項式 m に多項式演算である暗号化アルゴリズム E を施して、暗号文多項式 $c = E(m, r, h)$ を生成する。ここで、 $E(m, r, h)$ は、N T R U 暗号方式の暗号化アルゴリズム E に、平文多項式 m、乱数多項式 r 及び公開鍵多項式 h を入力して得られる多項式演算の結果である。暗号化アルゴリズム E については上記文献に詳しく述べられており、ここでは説明を省略する。

【 0 0 3 9 】

なお、NTRU暗号方式では、乱数多項式 r を生成するためのパラメータ d が予め決められており、乱数多項式 r は、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ他の係数は 0 となるように選ぶ。すなわち、乱数多項式 r は $N-1$ 次元以下の多項式であり、0 次元（定数項）から $N-1$ 次元まで、 N 個の係数があるが、この N 個の係数のうち、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ $(N-2d)$ 個の係数は 0 となるように選ぶ。上記文献によれば、パラメータ N が $N=167$ の場合、 $d=18$ である。すなわち、18 個の係数が 1 であり、かつ 18 個の係数が -1 であり、 $131 (=167-36)$ 個の係数が 0 となるように乱数多項式 r を選ぶ。

【0040】

復号化時には、秘密鍵多項式 f を用いて、暗号文多項式 c に多項式演算である復号アルゴリズム D を施して、復号文多項式 $m' = D(c, f)$ を生成する。ここで、 $D(c, f)$ は、NTRU暗号方式の復号アルゴリズム D に、暗号文多項式 c 、及び秘密鍵多項式 f を入力して得られる多項式演算の結果である。復号アルゴリズム D については上記文献に詳しく述べられており、ここでは説明を省略する。

【0041】

ところで、このNTRU暗号方式は、復号文多項式 m' が平文多項式 m と異なる場合が発生する。この場合は、復号時に正しく平文多項式 m が得られないことになる。このことを復号エラーが発生するという。復号エラーは、乱数多項式 r 、平文多項式 m 、公開鍵多項式 h 、秘密鍵多項式 f の組み合わせにより、発生するかどうかが決まる。具体的には、公開鍵多項式 h は、秘密鍵多項式 f とランダム多項式 g との演算結果により生成されるが、この公開鍵多項式 h を生成したときに用いたランダム多項式 g 、乱数多項式 r 、平文多項式 m 、秘密鍵多項式 f の演算結果の多項式 $(p \cdot r \times g + f \times m)$ の係数の値が $-q/2$ から $q/2$ の間に入らなかったとき、復号エラーが発生する。この復号エラーの発生を完全に避ける手法は現在知られていないが、上記文献によれば、 $N=167$ の場合、 $d=18$ とすれば、確率的にほとんど復号エラーは発生せず、実用上問題ないことが明記されている。

【 0 0 4 2 】

(実施の形態 1)

本発明の実施の形態 1 における暗号システム 1 の全体構成を図 1 に示す。この暗号システム 1 は平文多項式 m の暗号化通信を行うシステムであり、送信装置 1 1 0 と複数の受信装置 1 2 0 a、1 2 0 b、1 2 0 c とから構成され、送信装置 1 1 0 と受信装置 1 2 0 a、1 2 0 b、1 2 0 c とは通信路 1 3 0 を介して接続されている。

【 0 0 4 3 】

以下に、送信装置 1 1 0 は複数の受信装置のうち受信装置 1 2 0 a と暗号化通信を行うとし、これらの構成要素について詳細に説明を行う。

【 0 0 4 4 】

送信装置 1 1 0 は、図 2 に示すように、平文入力部 1 1 1、パラメータ記憶部 1 1 2、タイマ部 1 1 3、パラメータ制御部 1 1 4、乱数生成部 1 1 5、暗号化部 1 1 6、送信部 1 1 7 及び鍵更新部 1 1 8 から構成される。

【 0 0 4 5 】

平文入力部 1 1 1 は、外部より入力された平文多項式 m を暗号化部 1 1 6 に出力する。

【 0 0 4 6 】

パラメータ記憶部 1 1 2 は、図 3 に示すように、受信装置 1 2 0 a の固有番号 $ID a$ 、公開鍵多項式 $h a$ 及び乱数パラメータ $d a$ を、一組のデータ $DT a = (ID a, h a, d a)$ として記憶している（受信装置 1 2 0 b、1 2 0 c についても同様に $DT b = (ID b, h b, d b)$ 、 $DT c = (ID c, h c, d c)$ を記憶している）。ここで、乱数パラメータ $d a$ は、暗号化時に用いる乱数多項式 r を生成するためのパラメータであり、乱数多項式 r の係数のうち、係数が 1 であるものの数、及び係数が -1 であるものの数である。なお、乱数パラメータ $d a$ の初期値は、 $d a = 18$ とする。

【 0 0 4 7 】

タイマ部 1 1 3 は、一日毎に時間信号を発生し、パラメータ制御部 1 1 4 に入力する。

【 0 0 4 8 】

パラメータ制御部 1 1 4 は、タイマ部 1 1 3 から時間信号を受け取ったら、パラメータ記憶部 1 1 2 に記憶された乱数パラメータ $d a$ の値を 1 ずつ増加させる（乱数パラメータ $d b$ 、 $d c$ の値も、同様に 1 ずつ増加させる）。

【 0 0 4 9 】

乱数生成部 1 1 5 は、パラメータ記憶部 1 1 2 から受信装置 1 2 0 a の乱数パラメータ $d a$ を読み出す。そして、読み出した乱数パラメータ $d a$ に基づき、 $d a$ 個の係数が 1 であり、かつ $d a$ 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r をランダムに生成する。そして、生成した乱数多項式 r を暗号化部 1 1 6 へ出力する。

【 0 0 5 0 】

暗号化部 1 1 6 は、予め N T R U 暗号方式の暗号アルゴリズム E を有している。

【 0 0 5 1 】

暗号化部 1 1 6 は、平文入力部 1 1 1 から平文多項式 m を受け取り、パラメータ記憶部 1 1 2 から受信装置 1 2 0 a の公開鍵多項式 $h a$ を読み出し、乱数生成部 1 1 5 から乱数多項式 r を受け取る。そして、暗号化部 1 1 6 は、乱数多項式 r と公開鍵多項式 $h a$ を用いて、平文多項式 m に前記暗号アルゴリズム E を施して暗号文多項式 $E(m, r, h a)$ を生成し、生成した暗号文多項式 $E(m, r, h a)$ を送信部 1 1 7 へ出力する。

【 0 0 5 2 】

送信部 1 1 7 は、暗号文多項式 $E(m, r, h a)$ を、通信路 1 3 0 を介して受信装置 1 2 0 a へ送信する。

【 0 0 5 3 】

鍵更新部 1 1 8 は、通信路 1 3 0 を介して受信装置 1 2 0 a、1 2 0 b、1 2 0 c から、固有番号と新たな公開鍵多項式を受信することができる。もしも、受信装置 1 2 0 a の固有番号 $I D a$ と公開鍵多項式 $h a'$ を受信した場合、鍵更新部 1 1 8 は、パラメータ記憶部 1 1 2 に記憶されている $D T a = (I D a, h a, d a)$ を、 $D T a' = (I D a, h a', d a')$ に更新する。ここで $d a'$

は、乱数パラメータの初期値であり $d a' = 18$ である（受信装置 120b、120c から受信した場合は、それぞれ、DTb を DTb'、DTc を DTc' に更新する）。

【0054】

以上に述べた送信装置 110 は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【0055】

以下に、送信装置 110 の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

【0056】

最初に、送信装置 110 の暗号化通信処理について、図 4 に示すフローチャートを用いて説明する。

【0057】

まず、乱数生成部 115 は、パラメータ記憶部 112 から受信装置 120a の乱数パラメータ $d a$ を読み出し（ステップ S101）、そして、読み出した乱数パラメータ $d a$ に基づき、 $d a$ 個の係数が 1 であり、かつ $d a$ 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r をランダムに生成し、生成した乱数多項式 r を暗号化部 116 へ出力する（ステップ S102）。

【0058】

次に、暗号化部 116 は、平文入力部 111 から平文多項式 m を受け取り、パラメータ記憶部 112 から受信装置 120a の公開鍵多項式 $h a$ を読み出し、乱数生成部 115 から乱数多項式 r を受け取り（ステップ S103）、そして、暗号化部 116 は、乱数多項式 r と公開鍵多項式 $h a$ を用いて、平文多項式 m に暗号アルゴリズム E を施して暗号文多項式 $E(m, r, h a)$ を生成し、生成した暗号文多項式 $E(m, r, h a)$ を送信部 117 へ出力する（ステップ S104）。

【0059】

次に、送信部 117 は、受け取った暗号文多項式 $E(m, r, h a)$ を、通信

路 130 を介して受信装置 120a へ送信して処理を終了する（ステップ S105）。

【0060】

次に、送信装置 110 の乱数パラメータ更新処理について、図 5 に示すフローチャートを用いて説明する。

【0061】

まず、パラメータ制御部 114 は、タイマ部 113 から時間信号を受け取ったら、ステップ S112 へ処理を移し、そうでなければ処理を終了する（ステップ S111）。

【0062】

そして、パラメータ制御部 114 は、パラメータ記憶部 112 に記憶された乱数パラメータ da の値を 1 ずつ増加させて（乱数パラメータ db、dc の値も、同様に 1 ずつ増加させる）、処理を終了する（ステップ S112）。

【0063】

次に、送信装置 110 の公開鍵更新処理について、図 6 に示すフローチャートを用いて説明する。

【0064】

まず、鍵更新部 118 は、受信装置 120a、120b、120c のいずれから、固有番号と新たな公開鍵を受信したら、ステップ S122 へ処理を移し、そうでなければ処理を終了する（ステップ S121）。

【0065】

そして、鍵更新部 118 は、パラメータ記憶部 112 に記憶されている $DTa = (IDa, ha, da)$ を、 $DTa' = (IDa, ha', da')$ に更新して処理を終了する（受信装置 120a から受信した場合。受信装置 120b、120c から受信した場合は、それぞれ、DTb を DTb'、DTc を DTc' に更新する）。ここで da' は、乱数パラメータの初期値であり $da' = 18$ である（ステップ S122）。

【0066】

受信装置 120a は、図 7 に示すように、受信部 121、秘密鍵記憶部 122

、復号化部 1 2 3、復号文出力部 1 2 4、鍵再生成部 1 2 5、及び入力部 1 2 6 から構成される。

【 0 0 6 7 】

受信部 1 2 1 は、送信装置 1 1 0 から通信路 1 3 0 を介して、暗号文多項式 $E(m, r, ha)$ を受信し、受信した暗号文多項式 $E(m, r, ha)$ を復号化部 1 2 3 へ出力する。

【 0 0 6 8 】

秘密鍵記憶部 1 2 2 は、受信装置 1 2 0 a の秘密鍵多項式 f_a を記憶している。

【 0 0 6 9 】

復号化部 1 2 3 は、暗号化部 1 1 6 が有する暗号アルゴリズム E の逆変換である、NTRU 暗号方式の復号アルゴリズム D を予め有している。

【 0 0 7 0 】

復号化部 1 2 3 は、受信部 1 2 1 から暗号文多項式 $E(m, r, ha)$ を受け取り、秘密鍵記憶部 1 2 2 から受信装置 1 2 0 a の秘密鍵多項式 f_a を読み出す。そして、復号化部 1 2 3 は、秘密鍵多項式 f_a を用いて、暗号文多項式 $E(m, r, ha)$ に前記復号アルゴリズム D を施して復号文多項式 $m' = D(E(m, r, ha), f_a)$ を生成し、生成した復号文多項式 m' を復号文出力部 1 2 4 へ出力する。

【 0 0 7 1 】

復号文出力部 1 2 4 は、復号化部 1 2 3 から復号文多項式 m' を受け取り、復号文多項式 m' を外部へ出力する。

【 0 0 7 2 】

鍵再生成部 1 2 5 は、入力部 1 2 6 を介して鍵再生成要求信号を受け取った場合、NTRU 暗号の秘密鍵多項式 f_a' 及び公開鍵多項式 h_a' を新たに再生成して、秘密鍵記憶部 1 2 2 に記憶されている秘密鍵多項式 f_a を新たに生成した秘密鍵多項式 f_a' に更新する。そして、受信装置 1 2 0 a の固有番号 ID_a と新たな公開鍵多項式 h_a' を、通信路 1 3 0 を介して送信装置 1 1 0 に送信する。

【 0 0 7 3 】

受信装置 1 2 0 a を扱うユーザは、受信装置 1 2 0 a の公開鍵多項式 $h a$ と秘密鍵多項式 $f a$ の再生成を指示する鍵再生成要求信号を入力部 1 2 6 に入力することができる。この鍵再生成要求信号は、復号文出力部 1 2 4 から出力された復号文多項式 m' が正しく得られない等の理由で、ユーザが公開鍵多項式 $h a$ と秘密鍵多項式 $f a$ の再生成のために入力する信号である。

【 0 0 7 4 】

入力部 1 2 6 は、外部から入力された鍵再生成要求信号を鍵再生成部 1 2 5 に出力する。

【 0 0 7 5 】

以上に述べた受信装置 1 2 0 a は、以下に述べる復号化处理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【 0 0 7 6 】

以下に、送信装置 1 2 0 a の動作について、復号化处理、鍵更新処理に分けて説明を行う。

【 0 0 7 7 】

最初に、受信装置 1 2 0 a の復号化处理について、図 8 に示すフローチャートを用いて説明する。

【 0 0 7 8 】

まず、受信部 1 2 1 は、送信装置 1 1 0 から通信路 1 3 0 を介して、暗号文多項式 $E(m, r, h a)$ を受信し、受信した暗号文多項式 $E(m, r, h a)$ を復号化部 1 2 3 へ出力する（ステップ S 1 5 1）。

【 0 0 7 9 】

次に、復号化部 1 2 3 は、受信部 1 2 1 から暗号文多項式 $E(m, r, h a)$ を受け取り、秘密鍵記憶部 1 2 2 から受信装置 1 2 0 a の秘密鍵多項式 $f a$ を読み出し（ステップ S 1 5 2）、そして、復号化部 1 2 3 は、秘密鍵多項式 $f a$ を用いて、暗号文多項式 $E(m, r, h a)$ に復号アルゴリズム D を施して復号文多項式 $m' = D(E(m, r, h a), f a)$ を生成し、生成した復号文多項式 m' を復号文出力部 1 2 4 へ出力する（ステップ S 1 5 3）。

【 0 0 8 0 】

次に、復号文出力部 1 2 4 は、復号化部 1 2 3 から復号文多項式 m' を受け取り、復号文多項式 m' を外部へ出力して処理を終了する（ステップ S 1 5 4）。

【 0 0 8 1 】

次に、受信装置 1 2 0 a の鍵更新処理について、図 9 に示すフローチャートを用いて説明する。

【 0 0 8 2 】

まず、鍵再生成部 1 2 5 は、もしも、入力部 1 2 6 を介して鍵再生成要求信号を受け取ったら、ステップ S 1 6 2 へ処理を移し、そうでなければ処理を終了する（ステップ S 1 6 1）。

【 0 0 8 3 】

そして、鍵再生成部 1 2 5 は、NTRU 暗号の秘密鍵多項式 $f a'$ 及び公開鍵多項式 $h a'$ を新たに再生成して、秘密鍵記憶部 1 2 2 に記憶されている秘密鍵多項式 $f a$ を新たに生成した秘密鍵多項式 $f a'$ に更新し（ステップ S 1 6 2）、受信装置 1 2 0 a の固有番号 $I D a$ と新たな公開鍵多項式 $h a'$ を、通信路 1 3 0 を介して送信装置 1 1 0 に送信して処理を終了する（ステップ S 1 6 3）。

【 0 0 8 4 】

以下に、実施の形態 1 における暗号システム 1 全体の動作について説明する。

【 0 0 8 5 】

今、暗号システム 1 において、送信装置 1 1 0 は複数の受信装置のうち受信装置 1 2 0 a と暗号化通信を行うとする。

【 0 0 8 6 】

まず、送信装置 1 1 0 は、受信装置 1 2 0 a の固有番号 $I D a$ 、公開鍵多項式 $h a$ 及び乱数パラメータ $d a$ を、データ $D T a = (I D a, h a, d b)$ としてパラメータ記憶部 1 1 2 に記憶している（受信装置 1 2 0 b、1 2 0 c についても同様に $D T b = (I D b, h b, d b)$ 、 $D T c = (I D c, h c, d c)$ を記憶している）。乱数パラメータ $d a$ 、 $d b$ 、 $d c$ の初期値は、 $d a = d b = d c = 1 8$ である。

【 0 0 8 7 】

そして、送信装置 1 1 0 は暗号化通信処理に従って、平文多項式 m を暗号化して暗号文多項式 $E(m, r, h a)$ を生成し、生成した暗号文多項式 $E(m, r, h a)$ を通信路 1 3 0 を介して受信装置 1 2 0 a に送信する。一方、受信装置 1 2 0 a は前述した復号化処理に従って、暗号文多項式 $E(m, r, h a)$ を通信路 1 3 0 を介して送信装置 1 1 0 から受信し、受信した暗号文多項式 $E(m, r, h a)$ を復号して復号文多項式 m' を出力する。

【 0 0 8 8 】

なお、送信装置 1 1 0 では、乱数パラメータ更新処理に従って、タイマ部 1 1 3 が一日毎に発生する時間信号に応じて、パラメータ制御部 1 1 4 は、パラメータ記憶部 1 1 2 に記憶された全ての乱数パラメータ $d a$ 、 $d b$ 、 $d c$ の値を 1 ずつ増加させる。すなわち、パラメータ記憶部 1 1 2 に記憶された全ての乱数パラメータの値は一日毎に増加する。

【 0 0 8 9 】

従って、この送信装置 1 1 0 の暗号化通信処理が継続して行われると、暗号文多項式 $E(m, r, h a)$ を生成される際に用いられる乱数多項式 r は、係数が 1 であるもの、及び係数が -1 であるものの数が一日毎に増加する。

【 0 0 9 0 】

今、図 1 0 は、乱数パラメータ d の値に対し、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r を用いた場合の、NTRU 暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータ $d a$ の初期値 $d a = 1 8$ においては、送信装置 1 1 0 が生成する暗号文多項式 $E(m, r, h a)$ は、ほとんど復号エラーは発生しない（受信装置 1 2 0 は受信した暗号文多項式 $E(m, r, h a)$ から、平文多項式 m と等しい復号文多項式 m' を得ることができる）。一方で、期間が経過すれば、乱数パラメータ $d a$ が一日毎に徐々に大きくなるので、送信装置 1 1 0 が生成する暗号文多項式 $E(m, r, h a)$ は、徐々に復号エラー発生確率が大きくなる（受信装置 1 2 0 は受信した暗号文多項式 $E(m, r, h a)$ から、平文多項式 m と等しい復号文多項式 m' を得ることが徐々にできなくなる）。

【 0 0 9 1 】

そして、もしも受信装置 1 2 0 が平文多項式 m と等しい復号文多項式 m' を得る確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置 1 2 0 a を扱うユーザは、鍵更新処理を行うことにより、受信装置 1 2 0 a の公開鍵多項式 h_a と秘密鍵多項式 f_a の再生成を指示する鍵再生成要求信号を入力部 1 2 6 に入力することができる。すると、送信装置 1 1 0 の公開鍵更新処理により、パラメータ記憶部 1 1 2 の乱数パラメータ d_a は初期値 $d_a' = 18$ に更新されるので、復号エラー発生確率が元に戻り、再び受信装置 1 2 0 a は実用的に暗号化通信を行うことができるようになる。

【 0 0 9 2 】

実施の形態 1 では、送信装置 1 1 0 が暗号化通信時に用いる乱数多項式 r を、期間が経過するにつれて、係数が 1 であるもの、及び係数が -1 であるものの数を増加させるようにしている。これにより、受信装置 1 2 0 a の有する秘密鍵多項式 f_a が暴露されたとしても、暴露された秘密鍵多項式 f_a を不正に用いる第三者の受信装置では、期間が経過するにつれて、復号エラーの発生確率が大きくなり、送信装置 1 1 0 が行う暗号化通信を正しく復号できなくなる。この結果、この暗号システム 1 は、従来技術と異なり、秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することができるようになる。

【 0 0 9 3 】

また、正規に秘密鍵多項式 f_a を有する受信装置 1 2 0 a においても、期間が経過するにつれて、同じ秘密鍵多項式 f_a を使い続けると、徐々に復号エラーの発生確率が大きくなり、送信装置 1 1 0 が行う暗号化通信を正しく復号できなくなる。そして、受信装置 1 2 0 a を扱うユーザに、同じ秘密鍵多項式 f_a を使い続けると、復号エラーの発生確率が大きくなっていき、鍵を更新しないと暗号化通信が実用にならなくなることを知らしめ、鍵の更新のために受信装置 1 2 0 の入力部 1 2 6 を介して、鍵再生成要求信号を入力することを促すことができる。この結果、この暗号システム 1 は、従来技術と異なり、受信装置又は受信装置を扱う人に、鍵の更新を促すことができるようになる。

【 0 0 9 4 】

さらに、この暗号システム 1 は、従来技術と異なり、第三者機関による C R L や S R M を必要としない。

【 0 0 9 5 】

(実施の形態 2)

本発明の実施の形態 2 における暗号システム 2 は、暗号システム 1 を基本にして構成した、映画や音楽などのデジタル著作物（以降、コンテンツと呼ぶ）の配信に適した暗号システムである。

【 0 0 9 6 】

平文多項式 m を N T R U 暗号で暗号化して送信する代わりに、デジタルデータであるコンテンツ $C N T_i$ ($1 \leq i \leq k$) を暗号鍵 K_i ($1 \leq i \leq k$) を用いて共通鍵暗号で暗号化し、その暗号鍵 K_i ($1 \leq i \leq k$) を N T R U 暗号で暗号化して、暗号化したコンテンツと暗号化した暗号鍵を送信する点が暗号システム 1 と異なる。また、鍵サーバを利用して鍵の更新を行う点が暗号システム 1 と異なる。以下に詳細を説明する。

【 0 0 9 7 】

実施の形態 2 における暗号システム 2 の全体構成を図 1 1 に示す。この暗号システム 2 はコンテンツ $C N T$ の配信を行うシステムであり、コンテンツサーバ 2 1 0 と、鍵サーバ 2 2 0 と、受信装置 2 3 0 とから構成され、コンテンツサーバ 2 1 0 と受信装置 2 3 0 はインターネット 2 4 0 を介して接続されており、コンテンツサーバ 2 1 0 と鍵サーバ 2 2 0 は専用回線 2 5 0 で接続されており、鍵サーバ 2 2 0 と受信装置 2 3 0 とは、電話回線 2 6 0 で接続されている。

【 0 0 9 8 】

コンテンツサーバ 2 1 0 は、コンテンツ $C N T$ をユーザ j に提供する業者が有しており、鍵サーバ 2 2 0 は、コンテンツ $C N T$ を利用するための復号鍵をユーザ j に提供する業者が有しており、受信装置 2 3 0 は、コンテンツ $C N T$ を利用するユーザ j が有している。

【 0 0 9 9 】

以下に、これらの構成要素について詳細に説明を行う。

【 0 1 0 0 】

コンテンツサーバ 2 1 0 は、図 1 2 に示すように、コンテンツ記憶部 2 1 1、パラメータ記憶部 2 1 2、タイマ部 2 1 3、パラメータ制御部 2 1 4、乱数生成部 2 1 5、暗号鍵生成部 2 1 6、暗号化部 2 1 7、送信部 2 1 8 及び鍵更新部 2 1 9 から構成される。

【 0 1 0 1 】

コンテンツ記憶部 2 1 1 は、外部より入力されたコンテンツ CNT を、例えば一定時間毎に区切った MPEG 2 データ CNT i ($1 \leq i \leq k$) として格納している。

【 0 1 0 2 】

パラメータ記憶部 2 1 2 は、図 1 3 に示すように、ユーザ j 毎に、受信装置 2 3 0 の固有番号 ID j 、公開鍵多項式 h_j 及び乱数パラメータ d_j を、一組のデータ DT $j = (ID_j, h_j, d_j)$ ($1 \leq j \leq n$) として記憶している。ここで、乱数パラメータ d_j は、暗号化時に用いる乱数多項式 r_i ($1 \leq i \leq k$) を生成するためのパラメータであり、乱数多項式 r_i ($1 \leq i \leq k$) の係数のうち、係数が 1 であるものの数、及び係数が -1 であるものの数である。なお、乱数パラメータ d_j の初期値は、 $d_j = 18$ とする。

【 0 1 0 3 】

タイマ部 2 1 3 は、一日毎に時間信号を発生し、パラメータ制御部 2 1 4 に入力する。

【 0 1 0 4 】

パラメータ制御部 2 1 4 は、タイマ部 2 1 3 から時間信号を受け取ったら、パラメータ記憶部 2 1 2 に記憶されたデータ DT j の乱数パラメータ d_j ($1 \leq j \leq n$) の値を 1 ずつ増加させる。

【 0 1 0 5 】

乱数生成部 2 1 5 は、パラメータ記憶部 2 1 2 から送信装置 2 3 0 の乱数パラメータ d_j を読み出す。そして、読み出した乱数パラメータ d_j に基づき、 d_j 個の係数が 1 であり、かつ d_j 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r_i ($1 \leq i \leq k$) をランダムに生成する。そして、生成した乱数多項式 r_i ($1 \leq i \leq k$) を暗号化部 2 1 7 へ出力する。

【 0 1 0 6 】

暗号鍵生成部 2 1 6 は、ランダムに暗号鍵 K_i ($1 \leq i \leq k$) を生成し、暗号化部 2 1 7 へ出力する。

【 0 1 0 7 】

暗号化部 2 1 7 は、予め N T R U 暗号方式の暗号アルゴリズム E と、例えば D E S 暗号方式のような共通鍵暗号アルゴリズム $S y m$ を有している。

【 0 1 0 8 】

共通鍵暗号では、暗号鍵 K を用いて、平文 m に共通鍵暗号アルゴリズム $S y m$ を施して、暗号文 $c = S y m(m, K)$ を生成し、暗号鍵 K を用いて、暗号文 c に共通鍵暗号アルゴリズム $S y m$ を施して、復号文 $m' = S y m(c, K)$ を生成する。ここで、暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K が同一であれば、 $m' = m$ となる。なお、共通鍵暗号及び D E S 暗号方式については、非特許文献 1 に詳しく述べられているため、ここでの詳細な説明は省略する。

【 0 1 0 9 】

暗号化部 2 1 7 は、暗号鍵生成部 2 1 6 から暗号鍵 K_i ($1 \leq i \leq k$) を受け取り、受け取った暗号鍵 K_i ($1 \leq i \leq k$) を N T R U 暗号で暗号化できるように暗号鍵多項式 $K P_i$ ($1 \leq i \leq k$) に変換する。この変換は、暗号鍵 K_i をビット列としたとき、例えば、暗号鍵 K_i の下位 b ビット目の値を X^b の係数として暗号鍵多項式 $K P_i$ を構成することで実現できる。すなわち、 $K_i = 1 0 0 1 0$ (ビット表現) の場合、 $K P_i = X^5 + X^2$ となる。

【 0 1 1 0 】

そして、暗号化部 2 1 7 は、パラメータ記憶部 2 1 2 から受信装置 2 3 0 の公開鍵多項式 h_j を読み出し、乱数生成部 2 1 5 から乱数多項式 r_i ($1 \leq i \leq k$) を受け取る。そして、暗号化部 2 1 7 は、乱数多項式 r_i ($1 \leq i \leq k$) と公開鍵多項式 h_j を用いて、変換した暗号鍵多項式 $K P_i$ ($1 \leq i \leq k$) に N T R U 暗号方式の暗号アルゴリズム E を施して、暗号化暗号鍵多項式 $E K P_i = E(K P_i, r_i, h_j)$ ($1 \leq i \leq k$) を生成する。

【 0 1 1 1 】

そして、暗号化部 2 1 7 は、コンテンツ記憶部 2 1 1 から、コンテンツ CNT_i ($1 \leq i \leq k$) を受け取り、前記暗号鍵 K_i ($1 \leq i \leq k$) を使用して、コンテンツ CNT_i ($1 \leq i \leq k$) に共通鍵暗号アルゴリズム Sym を施して、暗号化コンテンツ $EC_i = Sym(CNT_i, K_i)$ ($1 \leq i \leq k$) を生成する。

【 0 1 1 2 】

そして、暗号化部 2 1 7 は、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を送信部 2 1 8 へ出力する。

【 0 1 1 3 】

送信部 2 1 8 は、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を、インターネット 2 4 0 を介して受信装置 2 3 0 へ送信する。

【 0 1 1 4 】

鍵更新部 2 1 9 は、専用回線 2 5 0 を介して鍵サーバ 2 2 0 から、受信装置 2 3 0 の固有番号 ID_j と公開鍵多項式 h_j' ($1 \leq j \leq n$) を受信することができる。もしも、受信装置 2 3 0 の固有番号 ID_j と公開鍵多項式 h_j' ($1 \leq j \leq n$) を受信した場合、鍵更新部 2 1 9 は、パラメータ記憶部 2 1 2 に記憶されているデータ $DT_j = (ID_j, h_j, d_j)$ を、 $DT_j' = (ID_j, h_j', d_j')$ に更新する。ここで d_j' は、乱数パラメータ d_j の初期値であり、 $d_j' = 18$ である。

【 0 1 1 5 】

以上に述べたコンテンツサーバ 2 1 0 は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【 0 1 1 6 】

以下に、コンテンツサーバ 2 1 0 の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

【 0 1 1 7 】

最初に、コンテンツサーバ 2 1 0 の暗号化通信処理について、図 1 4 に示すフローチャートを用いて説明する。

【0 1 1 8】

まず、乱数生成部 2 1 5 は、パラメータ記憶部 2 1 2 から受信装置 2 3 0 の乱数パラメータ d_j を読み出し（ステップ S 2 0 1）、そして、読み出した乱数パラメータ d_j に基づき、 d_j 個の係数が 1 であり、かつ d_j 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r_i ($1 \leq i \leq k$) をランダムに生成し、生成した乱数多項式 r_i ($1 \leq i \leq k$) を暗号化部 2 1 7 へ出力する（ステップ S 2 0 2）。

【0 1 1 9】

次に、暗号鍵生成部 2 1 6 は、ランダムに暗号鍵 K_i ($1 \leq i \leq k$) を生成し、生成した暗号鍵 K_i ($1 \leq i \leq k$) を暗号化部 2 1 7 へ出力する（ステップ S 2 0 3）。

【0 1 2 0】

次に、暗号化部 2 1 7 は、暗号鍵生成部 2 1 6 から暗号鍵 K_i ($1 \leq i \leq k$) を受け取り、受け取った暗号鍵 K_i ($1 \leq i \leq k$) を NTRU 暗号で暗号化できるように暗号鍵多項式 KP_i ($1 \leq i \leq k$) に変換し（ステップ S 2 0 4）、そして、コンテンツ記憶部 2 1 1 からコンテンツ CNT_i ($1 \leq i \leq k$) を読み出し、パラメータ記憶部 2 1 2 から受信装置 2 3 0 の公開鍵多項式 h_j を読み出し、乱数生成部 2 1 5 から乱数多項式 r_i ($1 \leq i \leq k$) を受け取る（ステップ S 2 0 5）。そして、暗号化部 2 1 7 は、乱数多項式 r_i ($1 \leq i \leq k$) と公開鍵多項式 h_j を用いて、変換した暗号鍵多項式 KP_i ($1 \leq i \leq k$) に NTRU 暗号方式の暗号アルゴリズム E を施して、暗号化暗号鍵多項式 $EKP_i = E(KP_i, r_i, h_j)$ ($1 \leq i \leq k$) を生成する（ステップ S 2 0 6）。そして、暗号化部 2 1 7 は、コンテンツ記憶部 2 1 1 から、コンテンツ CNT_i ($1 \leq i \leq k$) を受け取り、前記暗号鍵 K_i ($1 \leq i \leq k$) を使用して、コンテンツ CNT_i ($1 \leq i \leq k$) に共通鍵暗号アルゴリズム Sym を施して、暗号化コンテンツ $EC_i = Sym(CNT_i, K_i)$ ($1 \leq i \leq k$) を生成し（ステップ S 2 0 7）、そして、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を送信部 2 1 8 へ出力する（ステップ S 2 0 8）。

【0 1 2 1】

次に、送信部 2 1 8 は、受け取った暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) と暗号化コンテンツ $E C_i$ ($1 \leq i \leq k$) をインターネット 2 4 0 を介して受信装置 2 3 0 へ送信して処理を終了する (ステップ S 2 0 9)。

【 0 1 2 2 】

次に、コンテンツサーバ 2 1 0 の乱数パラメータ更新処理について、図 1 5 に示すフローチャートを用いて説明する。

【 0 1 2 3 】

まず、パラメータ制御部 2 1 4 は、タイマ部 2 1 3 から時間信号を受け取ったら、ステップ S 2 1 2 へ処理を移し、そうでなければ処理を終了する (ステップ S 2 1 2)。

【 0 1 2 4 】

そして、パラメータ制御部 2 1 4 は、パラメータ記憶部 2 1 2 に記憶されている乱数パラメータ d_j ($1 \leq j \leq n$) を 1 ずつ増加させて、処理を終了する (ステップ S 2 1 2)。

【 0 1 2 5 】

次に、コンテンツサーバ 2 1 0 の公開鍵更新処理について、図 1 6 に示すフローチャートを用いて説明する。

【 0 1 2 6 】

まず、鍵更新部 2 1 9 は、専用回線 2 5 0 を介して鍵サーバ 2 2 0 から、受信装置 2 3 0 の固有番号 $I D_j$ と公開鍵多項式 h_j' ($1 \leq j \leq n$) を受信したら、ステップ S 2 2 2 へ処理を移し、そうでなければ処理を終了する (ステップ S 2 2 1)。

【 0 1 2 7 】

そして、鍵更新部 2 1 9 は、パラメータ記憶部 2 1 2 に記憶されているデータ $D T_j = (I D_j, h_j, d_j)$ を、 $D T_j' = (I D_j, h_j', d_j')$ に更新して処理を終了する。ここで d_j' は、乱数パラメータ d_j の初期値であり、 $d_j' = 18$ である (ステップ S 2 2 2)。

【 0 1 2 8 】

鍵サーバ 2 2 0 は、図 1 7 に示すように、I D 受信部 2 2 1、鍵再生部 2 2

2、公開鍵送信部 223 及び秘密鍵送信部 224 から構成される。

【0129】

ID受信部 221 は、受信装置 230 から電話回線 260 を介して、受信装置 230 の固有番号 ID j ($1 \leq j \leq n$) を受信すると、受信した固有番号 ID j を鍵再生成部 222 に出力する。

【0130】

鍵再生成部 222 は、ID受信部 221 から固有番号 ID j を受け取ると、NTRU暗号方式の秘密鍵多項式 f_j' と公開鍵多項式 h_j' を生成し、受け取った固有番号 ID j と生成した公開鍵多項式 h_j' を公開鍵送信部 223 に出力し、生成した秘密鍵多項式 f_j' を秘密鍵送信部 224 に出力する。

【0131】

公開鍵送信部 223 は、鍵再生成部 222 から固有番号 ID j と公開鍵多項式 h_j' を受け取ると、受け取った固有番号 ID j と公開鍵多項式 h_j' を、専用回線 250 を介してコンテンツサーバ 210 へ送信する。

【0132】

秘密鍵送信部 224 は、鍵再生成部 222 から秘密鍵多項式 f_j' を受け取ると、受け取った秘密鍵多項式 f_j' を、電話回線 260 を介して受信装置 230 へ送信する。

【0133】

以上に述べた鍵サーバ 220 の動作について、図 18 に示すフローチャートを用いて説明する。

【0134】

ID受信部 221 は、受信装置 230 から電話回線 260 を介して、受信装置 230 の固有番号 ID j ($1 \leq j \leq n$) を受信したら、ステップ S232 へ処理を移し、そうでなければ処理を終了する（ステップ S231）。ID受信部 221 は、受信した固有番号 ID j を鍵再生成部 222 に出力する（ステップ S232）。

【0135】

次に、鍵再生成部 222 は、ID受信部 221 から固有番号 ID を受け取り、

NTRU暗号方式の秘密鍵多項式 f_j' と公開鍵多項式 h_j' を生成し、受け取った固有番号 ID_j と生成した公開鍵多項式 h_j' を公開鍵送信部 2 2 3 に出力し、生成した秘密鍵多項式 f_j' を秘密鍵送信部 2 2 4 に出力する（ステップ S 2 3 3）。

【0 1 3 6】

次に、公開鍵送信部 2 2 3 は、鍵再生成部 2 2 2 から固有番号 ID_j と公開鍵多項式 h_j' を受け取り、受け取った固有番号 ID_j と公開鍵多項式 h_j' を、専用回線 2 5 0 を介してコンテンツサーバ 2 1 0 へ送信する（ステップ S 2 3 4）。

【0 1 3 7】

次に、秘密鍵送信部 2 2 4 は、鍵再生成部 2 2 2 から秘密鍵多項式 f_j' を受け取り、受け取った秘密鍵多項式 f_j' を、電話回線 2 6 0 を介して受信装置 2 3 0 へ送信する（ステップ S 2 3 5）。

【0 1 3 8】

受信装置 2 3 0 は、図 1 9 に示すように、受信部 2 3 1、秘密鍵記憶部 2 3 2、復号化部 2 3 3、出力部 2 3 4、鍵更新用送受信部 2 3 5、及び入力部 2 3 6 から構成される。

【0 1 3 9】

受信部 2 3 1 は、コンテンツサーバ 2 1 0 からインターネット 2 4 0 を介して、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を受信し、受信した暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を復号化部 2 3 3 へ出力する。

【0 1 4 0】

秘密鍵記憶部 2 3 2 は、受信装置 2 3 0 の秘密鍵多項式 f_j を記憶している。

【0 1 4 1】

復号化部 2 3 3 は、暗号化部 2 1 7 が有する暗号アルゴリズム E の逆変換である、NTRU暗号方式の復号アルゴリズム D と、暗号化部 2 1 7 が有する共通鍵暗号アルゴリズム Sym を予め有している。

【0 1 4 2】

復号化部 2 3 3 は、受信部 2 3 1 から暗号化暗号鍵多項式 $E K P i$ ($1 \leq i \leq k$) と暗号化コンテンツ $E C i$ ($1 \leq i \leq k$) を受け取り、秘密鍵記憶部 2 3 2 から受信装置 2 3 0 の秘密鍵多項式 $f j$ を読み出す。そして、復号化部 2 3 3 は、秘密鍵多項式 $f j$ を用いて、暗号化暗号鍵多項式 $E K P i$ ($1 \leq i \leq k$) に前記復号アルゴリズム D を施して、復号暗号鍵多項式 $K P i' = D(E K P i, f j)$ ($1 \leq i \leq k$) を生成する。

【 0 1 4 3 】

そして、復号化部 2 3 3 は、コンテンツサーバ 2 1 0 の暗号化部 2 1 7 における変換の逆変換を用いて、復号暗号鍵多項式 $K P i$ ($1 \leq i \leq k$) を復号暗号鍵 $K i$ ($1 \leq i \leq k$) に変換する。

【 0 1 4 4 】

そして、復号化部 2 3 3 は、復号暗号鍵 $K i'$ ($1 \leq i \leq k$) を使用して、暗号化コンテンツ $E C i$ ($1 \leq i \leq k$) に共通鍵暗号アルゴリズム $S y m$ を施して、復号コンテンツ $C N T i' = S y m(E C i, K i')$ ($1 \leq i \leq k$) を生成し、復号コンテンツ $C N T i'$ ($1 \leq i \leq k$) を出力部 2 3 4 に出力する。

【 0 1 4 5 】

出力部 2 3 4 は、例えばモニタやスピーカ等を備えており、入力された復号コンテンツ $C N T i'$ ($1 \leq i \leq k$) を外部に出力する。

【 0 1 4 6 】

モニタは、復号コンテンツ $C N T i'$ ($1 \leq i \leq k$) の $M P E G 2$ データから得られる映像を外部に出力し、スピーカ 3 3 5 は、復号コンテンツ $C N T i'$ ($1 \leq i \leq k$) の $M P E G 2$ データから得られる音声を外部に出力する。

【 0 1 4 7 】

鍵更新用送受信部 2 3 5 は、入力部 2 3 6 を介して鍵再生成要求信号を受け取った場合、受信装置 2 3 0 の固有番号 $I D j$ を、電話回線 2 6 0 を介して鍵サーバ 2 2 0 へ送信し、鍵サーバ 2 2 0 から電話回線 2 6 0 を介して、秘密鍵多項式 $f j'$ を受信して、秘密鍵記憶部 2 3 2 に記憶されている秘密鍵多項式 $f j$ を受信した秘密鍵多項式 $f j'$ に更新する。

【 0 1 4 8 】

受信装置 2 3 0 を扱うユーザ j は、受信装置 2 3 0 の公開鍵多項式 h_j と秘密鍵多項式 f_j の再生成を指示する鍵再生成要求信号を入力部 3 3 5 に入力することができる。この鍵再生成要求信号は、出力部 2 3 4 から出力された復号コンテンツ CNT_i' ($1 \leq i \leq k$) が正しく得られない等の理由で、ユーザが公開鍵多項式 h_j と秘密鍵多項式 f_j の再生成のために入力する信号である。

【 0 1 4 9 】

入力部 2 3 6 は、外部から入力された鍵再生成要求信号を鍵更新用送受信部 2 3 5 に出力する。

【 0 1 5 0 】

以上に述べた受信装置 2 3 0 は、以下に述べる復号化处理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

【 0 1 5 1 】

以下に、受信装置 2 3 0 の動作について、復号化处理、鍵更新処理に分けて説明を行う。

【 0 1 5 2 】

最初に、受信装置 2 3 0 の復号化处理について、図 2 0 に示すフローチャートを用いて説明する。

【 0 1 5 3 】

まず、受信部 2 3 1 は、コンテンツサーバ 2 1 0 からインターネット 2 4 0 を介して、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を受信し、受信した暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を復号化部 2 3 3 へ出力する（ステップ S 2 5 1）。

【 0 1 5 4 】

次に、復号化部 2 3 3 は、受信部 2 3 1 から暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と暗号化コンテンツ EC_i ($1 \leq i \leq k$) を受け取り、秘密鍵記憶部 2 3 2 から受信装置 2 3 0 の秘密鍵多項式 f_j を読み出し（ステップ S 2 5 2）、そして、秘密鍵多項式 f_j を用いて、暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) に復号アルゴリズム D を施して、復号暗号鍵多項式 $KP_i' = D(EKP_i$

, f_j) ($1 \leq i \leq k$) を生成する (ステップ S253)。

【0155】

次に、復号化部 233 は、コンテンツサーバ 210 の暗号化部 217 における変換の逆変換を用いて、復号暗号鍵多項式 KP_i ($1 \leq i \leq k$) を復号暗号鍵 K_i ($1 \leq i \leq k$) に変換する (ステップ S254)。

【0156】

次に、復号化部 233 は、復号暗号鍵 K_i' ($1 \leq i \leq k$) を使用して、暗号化コンテンツ EC_i ($1 \leq i \leq k$) に共通鍵暗号アルゴリズム Sym を施して、復号コンテンツ $CNT_i' = Sym(EC_i, K_i')$ ($1 \leq i \leq k$) を生成し、復号コンテンツ CNT_i' ($1 \leq i \leq k$) を出力部 234 に出力する (ステップ S255)。

【0157】

次に、出力部 234 は、それぞれ、復号コンテンツ CNT_i' ($1 \leq i \leq k$) の MPEG2 データから得られる映像及び音声を外部に出力して処理を終了する (ステップ S256)。

【0158】

次に、受信装置 230 の鍵更新処理について、図 21 に示すフローチャートを用いて説明する。

【0159】

まず、鍵更新用送受信部 235 は、もしも、入力部 236 を介して鍵再生成要求信号を受け取ったら、ステップ S262 へ処理を移し、そうでなければ処理を終了する (ステップ S261)。

【0160】

次に、鍵更新用送受信部 235 は、受信装置 230 の固有番号 ID_j を、電話回線 260 を介して鍵サーバ 220 へ送信し (ステップ S262)、鍵サーバ 220 から電話回線 260 を介して、秘密鍵多項式 f_j' を受信して、秘密鍵記憶部 232 に記憶されている秘密鍵多項式 f_j を受信した秘密鍵多項式 f_j' に更新して処理を終了する (ステップ S263)。

【0161】

以下に、実施の形態 2 における暗号システム 2 全体の動作について暗号システム 1 との差異点を中心に説明する。

【0162】

まず、コンテンツサーバ 210 は、受信装置 230 の固有番号 ID_j 、公開鍵多項式 h_j 及び乱数パラメータ d_j を、データ $DT_j = (ID_j, h_j, d_j)$ としてパラメータ記憶部 212 に記憶している。乱数パラメータ d_j の初期値は、 $d_j = 18$ である。

【0163】

そして、コンテンツサーバ 210 は暗号化通信処理に従って、コンテンツ CNT_i ($1 \leq i \leq k$) を暗号鍵 K_i ($1 \leq i \leq k$) を用いて共通鍵暗号で暗号化して暗号化コンテンツ EC_i ($1 \leq i \leq k$) を生成し、その暗号鍵 K_i ($1 \leq i \leq k$) から変換した暗号鍵多項式 KP_i ($1 \leq i \leq k$) を NTRU 暗号で暗号化して暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) を生成し、暗号化コンテンツ EC_i ($1 \leq i \leq k$) を暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) と共にインターネット 240 を介して受信装置 230 に送信する。一方、受信装置 230 は復号化処理に従って、暗号化コンテンツ EC_i ($1 \leq i \leq k$) と暗号化暗号鍵 EK_i ($1 \leq i \leq k$) をインターネット 240 を介して送信装置 210 から受信し、受信した暗号化暗号鍵多項式 EKP_i ($1 \leq i \leq k$) を復号して復号暗号鍵多項式 KP_i' ($1 \leq i \leq k$) を生成し、これを変換した復号暗号鍵 K_i ($1 \leq i \leq k$) を用いて、暗号化コンテンツ EC_i ($1 \leq i \leq k$) を復号して復号コンテンツ CNT_i' ($1 \leq i \leq k$) を出力する。

【0164】

なお、コンテンツサーバ 210 では、乱数パラメータ更新処理に従って、タイマ部 213 が一日毎に発生する時間信号に応じて、パラメータ制御部 214 は、パラメータ記憶部 212 に記憶された全ての乱数パラメータ d_j ($1 \leq j \leq n$) の値を 1 ずつ増加させる。すなわち、パラメータ記憶部 212 に記憶された全ての乱数パラメータ d_j ($1 \leq i \leq n$) の値は一日毎に増加する。

【0165】

従って、このコンテンツサーバ 210 の暗号化通信処理が継続して行われると

、暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) を生成される際に用いられる乱数多項式 r_i ($1 \leq i \leq k$) は、係数が 1 であるもの、及び係数が -1 であるものの数が一日毎に増加する。

【0166】

今、図 10 は、乱数パラメータ d の値に対し、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r を用いた場合の、NTRU 暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータ d_j の初期値 $d_j = 18$ においては、コンテンツサーバ 210 が生成する暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) は、ほとんど復号エラーは発生しない（受信装置 230 は受信した暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) から暗号鍵 K_i と等しい復号暗号鍵 K_i' を得ることができて正しくコンテンツ CNT_i が復号できる）。一方で、期間が経過すれば、乱数パラメータ d_j が一日毎に徐々に大きくなるので、コンテンツサーバ 210 が生成する暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) は、徐々に復号エラー発生確率が大きくなる（受信装置 230 は受信した暗号化暗号鍵多項式 $E K P_i$ ($1 \leq i \leq k$) から暗号鍵 K_i と等しい復号暗号鍵 K_i' を得ることが徐々にできなくなり、コンテンツ CNT_i を徐々に正しく復号できなくなる）。

【0167】

そして、もしも受信装置 230 がコンテンツ CNT_i ($1 \leq i \leq k$) を正しく復号できる確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置 230 を扱うユーザ j は、鍵更新処理を行うことにより、受信装置 230 の公開鍵多項式 h_j と秘密鍵多項式 f_j の再生成を指示する鍵再生成要求信号を入力部 236 に入力することができる。すると、鍵サーバ 220 により、コンテンツサーバ 210 のパラメータ記憶部 212 の乱数パラメータ d_j は初期値 $d_j' = 18$ に更新されるので、復号エラー発生確率が元に戻り、再び受信装置 230 は実用的に暗号化通信を行うことができるようになる。

【0168】

実施の形態 2 では、デジタルデータであるコンテンツ CNT を一定時間毎に分割し、 CNT_i ($1 \leq i \leq k$) を受信装置 230 へ配信している。一般に、MP

EG2のようなデジタルデータの場合、復号エラーが発生して正しくCNT i が得られないと、動画像や音声にノイズが発生する。従って、期間が経過すると、復号エラーの発生確率が増加し、徐々に動画像や音声にノイズが増えることになる。これにより、コンテンツを提供する業者が、例えば1ヵ月間は実用上問題ないノイズ発生レベルでコンテンツをユーザに視聴させ、1ヵ月を過ぎると復号エラー発生確率が増加してノイズ発生レベルが大きくなり、鍵更新を行わない限りユーザがコンテンツを実用的に視聴できないようにさせることができる。すなわち、期間限定のコンテンツ配信に適する。

【0169】

また、一般に、MPEG2のようにサイズが大きいCNT i ($1 \leq i \leq k$) の場合、各CNT i を全てNTRU暗号で暗号化しようとする、NTRU暗号の入力ビット長に合わせてCNT i を分割し、複数回NTRU暗号の暗号処理を行わなければならない。しかし、この場合、暗号鍵K i をNTRU暗号で暗号化し、サイズの大きいコンテンツCNT i は公開鍵暗号に比べて速度の速い共通鍵暗号で暗号化するので、高速処理が可能であり、コンテンツ配信に適する。

【0170】

また、鍵の更新時に、鍵サーバ220を利用するので、鍵サーバ220でユーザ j の鍵更新の回数を把握することができ、この回数によりコンテンツを提供する業者がユーザ j にコンテンツ配信の課金を行うこともできる。

【0171】

なお、実施の形態1で得られる効果も同様に得られる。

【0172】

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0173】

用いるNTRU暗号のパラメータは $N = 167$ に限定されず、他のパラメータでもよい。

【0174】

パラメータ制御部 1 1 4、2 1 4 では、一日毎に乱数パラメータを 1 ずつ増加させる以外に、期間が経過するにつれて徐々に増加させれば、任意の期間毎に乱数パラメータを増加させてもよいし、またパラメータの増加分を任意にしてもよい。

【 0 1 7 5 】

さらに、パラメータ制御部 1 1 4、2 1 4 は、期間の経過に応じてではなく、乱数パラメータが読み出される毎に乱数パラメータを増加させてもよいし、乱数パラメータが読み出される回数に応じて乱数パラメータを増加させてもよい。これにより、暗号化回数が多くなるにつれ、徐々に復号エラー発生確率が大きくなるようにすることができるので、暴露された秘密鍵を有する第三者の受信装置に復号され続けることを防止でき、また受信装置又は受信装置を扱う人に鍵の更新を促すことができる。また、これにより、期間限定のコンテンツ配信以外にも、回数限定のコンテンツ配信にも利用できるようになる。

【 0 1 7 6 】

鍵再生成要求信号は入力部 1 2 6、2 3 6 を介して外部から入力される代わりに、受信装置 1 2 0、2 3 0、が何らかの方法で復号エラーを検知して、自動的に鍵再生成要求信号が入力されるようにしてもよい。

【 0 1 7 7 】

これは、例えば、実施の形態 2 における復号化部 2 3 3 が、さらに、復号コンテンツ $CNT i'$ が MPEG 2 のフォーマットに従っているかどうかを判別して復号エラーを検知し、復号エラー発生の度合いが大きくなったら鍵再生成要求信号を入力部 2 3 6 に入力することで実現できる。また、例えば、平文多項式 m や暗号鍵多項式 $KP i$ ($1 \leq i \leq k$) の高次の 10 次元分の係数を 1 とする等、そのフォーマットを定めておき、復号化部 1 2 3、2 2 3 が、さらに、復号文多項式 m' や復号暗号鍵多項式 $KP i'$ がそのフォーマットに従うかどうかを判別して復号エラーを検知し、復号エラー発生の度合いが大きくなったら鍵再生成要求信号を入力部 1 2 6、2 3 6 に入力することでも実現できる。

【 0 1 7 8 】

実施の形態 2 において、インターネット 2 4 0、専用回線 2 5 0、電話回線 2

60は、衛生通信網等の他の通信路を用いてもよいし、また同じ通信路を用いてもよい。なお、鍵サーバ220と受信装置230との間の通信路では、秘密鍵 f_j の送信が行われるので、安全性を高めるために暗号化通信を行ってもよい。

【0179】

実施の形態2において、共通鍵暗号アルゴリズムSymとして、AES暗号等の他の共通鍵暗号方式を用いてもよい。

【0180】

実施の形態2において、コンテンツCNT i ($1 \leq i \leq k$)は、MPEG2データに限らず、Windows (R) Media PlayerやReal Playerで再生可能なデジタルデータでもよいし、そのデータの形式は限られない。

【0181】

実施の形態2において、コンテンツサーバ210と鍵サーバ320は同一システム内にあってもよい。

【0182】

本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0183】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、CD-ROM、DVD-ROM、DVD-RAM等、に記録したものとしてもよい。

【0184】

上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0185】

【発明の効果】

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、暗号化通信にNTRU暗号方式を用い、送

信装置で乱数パラメータを期間が経過するにつれ増加させるようにしたので、期間が経過するにつれて、受信装置で暗号化通信を正しく復号できなくなるようにすることが可能となった。

【 0 1 8 6 】

これにより、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム又は送信装置を提供でき、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することが可能となった。

【 0 1 8 7 】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、復号を行うに従い、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることが可能となった。

【 0 1 8 8 】

さらに、送信装置が暗号化通信を行うに際して、第三者機関による C R L や S R M を必要としない暗号システム、送信装置又は受信装置を提供することが可能となった。

【 0 1 8 9 】

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価値は大きい。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における暗号システム 1 の構成を示す図

【図 2】

本発明の実施の形態 1 における送信装置 1 1 0 の構成を示す図

【図 3】

本発明の実施の形態 1 におけるパラメータ記憶部 1 1 2 の構成を示す図

【図 4】

本発明の実施の形態 1 における送信装置 1 1 0 の暗号化通信処理の流れを示すフローチャート

【図 5】

本発明の実施の形態 1 における送信装置 1 1 0 の乱数パラメータ更新処理の流れを示すフローチャート

【図 6】

本発明の実施の形態 1 における送信装置 1 1 0 の公開鍵更新処理の流れを示すフローチャート

【図 7】

本発明の実施の形態 1 における受信装置 1 2 0 a の構成を示す図

【図 8】

本発明の実施の形態 1 における受信装置 1 2 0 a の復号化処理の流れを示すフローチャート

【図 9】

本発明の実施の形態 1 における受信装置 1 2 0 a の鍵更新処理の流れを示すフローチャート

【図 1 0】

N T R U 暗号方式の復号エラー発生確率の測定結果を示す図

【図 1 1】

本発明の実施の形態 2 における暗号システム 2 の構成を示す図

【図 1 2】

本発明の実施の形態 2 におけるコンテンツサーバ 2 1 0 の構成を示す図

【図 1 3】

本発明の実施の形態 2 におけるパラメータ記憶部 2 1 2 の構成を示す図

【図 1 4】

本発明の実施の形態 2 におけるコンテンツサーバ 2 1 0 の暗号化通信処理の流れを示すフローチャート

【図 1 5】

本発明の実施の形態 2 におけるコンテンツサーバ 2 1 0 の乱数パラメータ更新

処理の流れを示すフローチャート

【図 1 6】

本発明の実施の形態 2 におけるコンテンツサーバ 2 1 0 の公開鍵更新処理の流れを示すフローチャート

【図 1 7】

本発明の実施の形態 2 における鍵サーバ 2 2 0 の構成を示す図

【図 1 8】

本発明の実施の形態 2 における鍵サーバ 2 2 0 の処理の流れを示すフローチャート

【図 1 9】

本発明の実施の形態 2 における受信装置 2 3 0 の構成を示す図

【図 2 0】

本発明の実施の形態 2 における受信装置 2 3 0 の復号化処理の流れを示すフローチャート

【図 2 1】

本発明の実施の形態 2 における受信装置 2 3 0 の鍵更新処理の流れを示すフローチャート

【符号の説明】

1, 2 暗号システム

1 1 0 送信装置

1 1 1 平文入力部

1 1 2, 2 1 2 パラメータ記憶部

1 1 3, 2 1 3 タイマ部

1 1 4, 2 1 4 パラメータ制御部

1 1 5, 2 1 5 乱数生成部

1 1 6, 2 1 7 暗号化部

1 1 7, 2 1 8 送信部

1 1 8, 2 1 9 鍵更新部

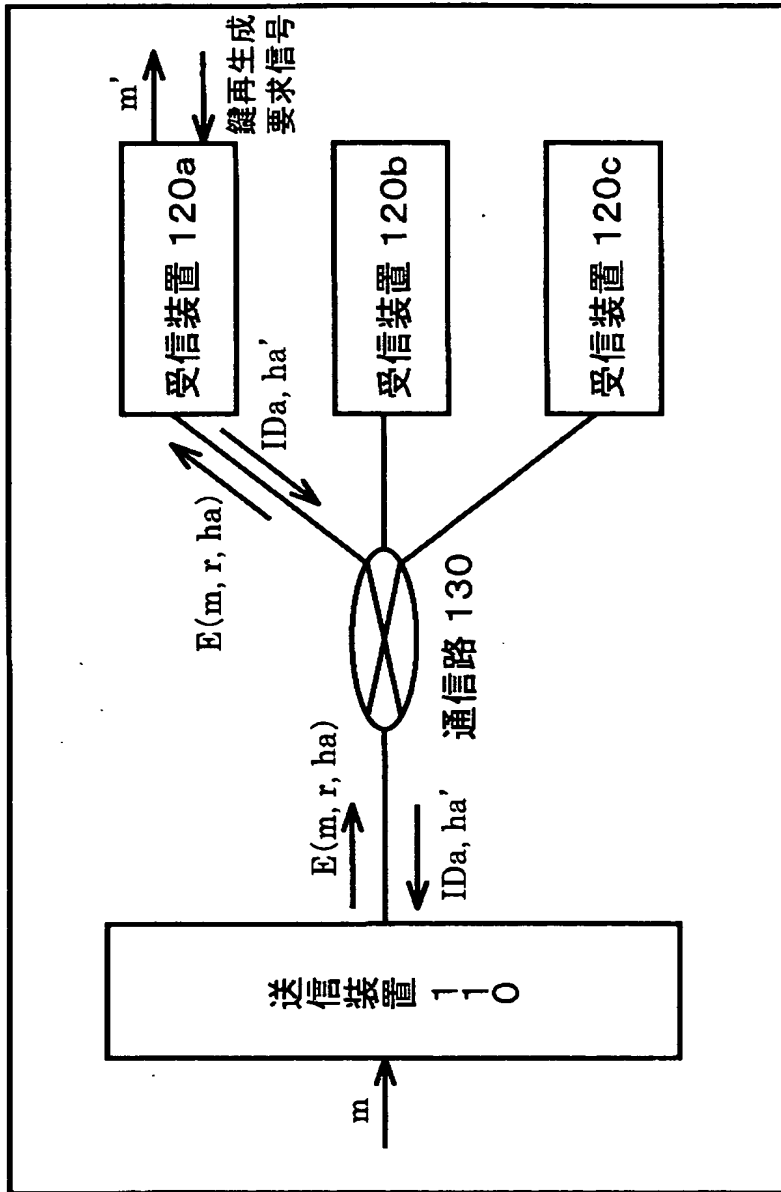
1 2 0 a, 1 2 0 b, 1 2 0 c, 2 3 0 受信装置

1 2 1, 2 3 1 受信部
1 2 2, 2 3 2 秘密鍵記憶部
1 2 3, 2 3 3 復号化部
1 2 4 復号文出力部
1 2 5, 2 2 2 鍵再生成部
1 2 6, 2 3 6 入力部
1 3 0 通信路
2 1 0 コンテンツサーバ
2 1 1 コンテンツ記憶部
2 1 6 暗号鍵生成部
2 2 0 鍵サーバ
2 2 1 I D 受信部
2 2 3 公開鍵送信部
2 2 4 秘密鍵送信部
2 3 4 出力部
2 3 5 鍵更新用送受信部
2 4 0 インターネット
2 5 0 専用回線
2 6 0 電話回線

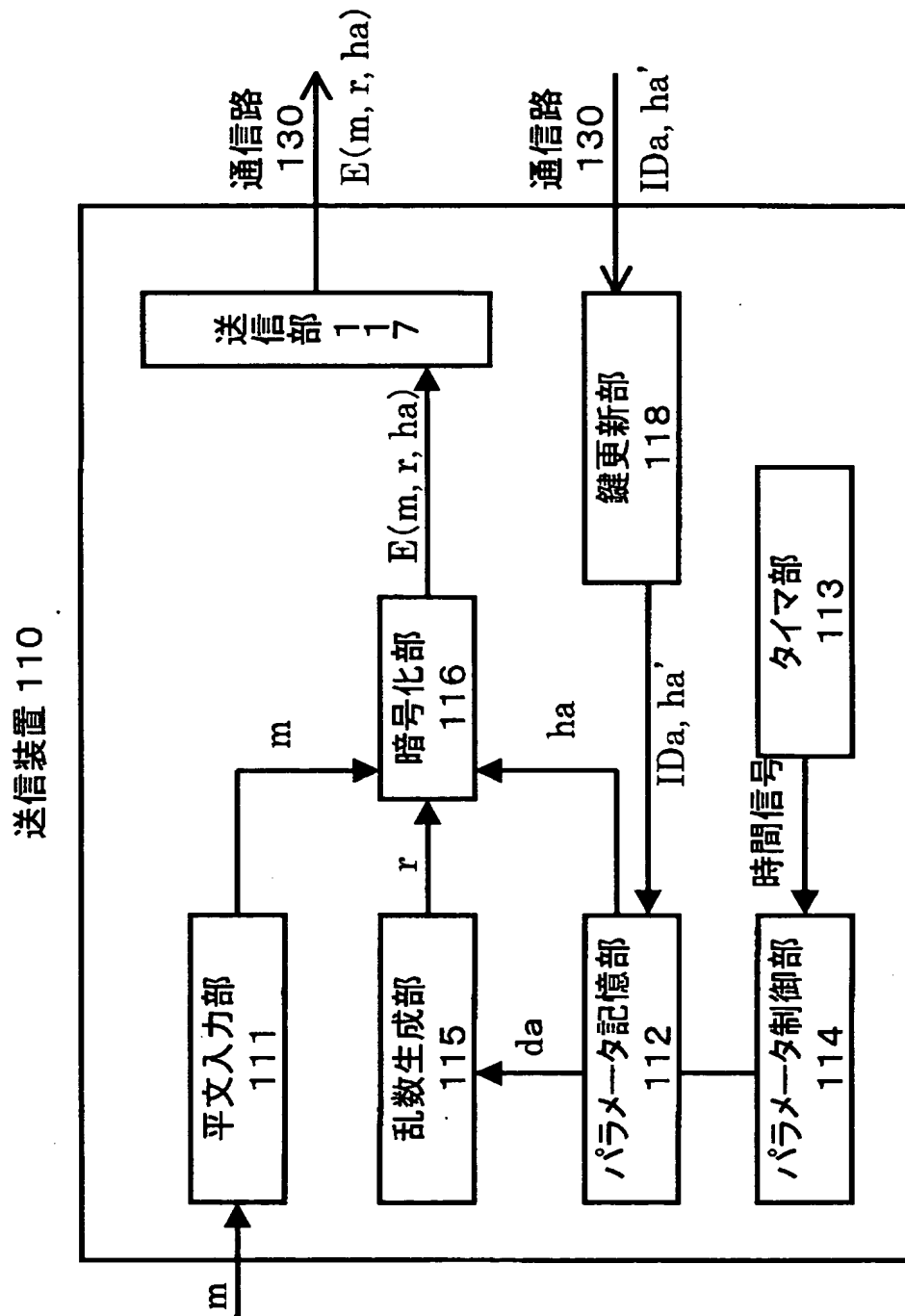
【書類名】 図面

【図 1】

暗号システム 1

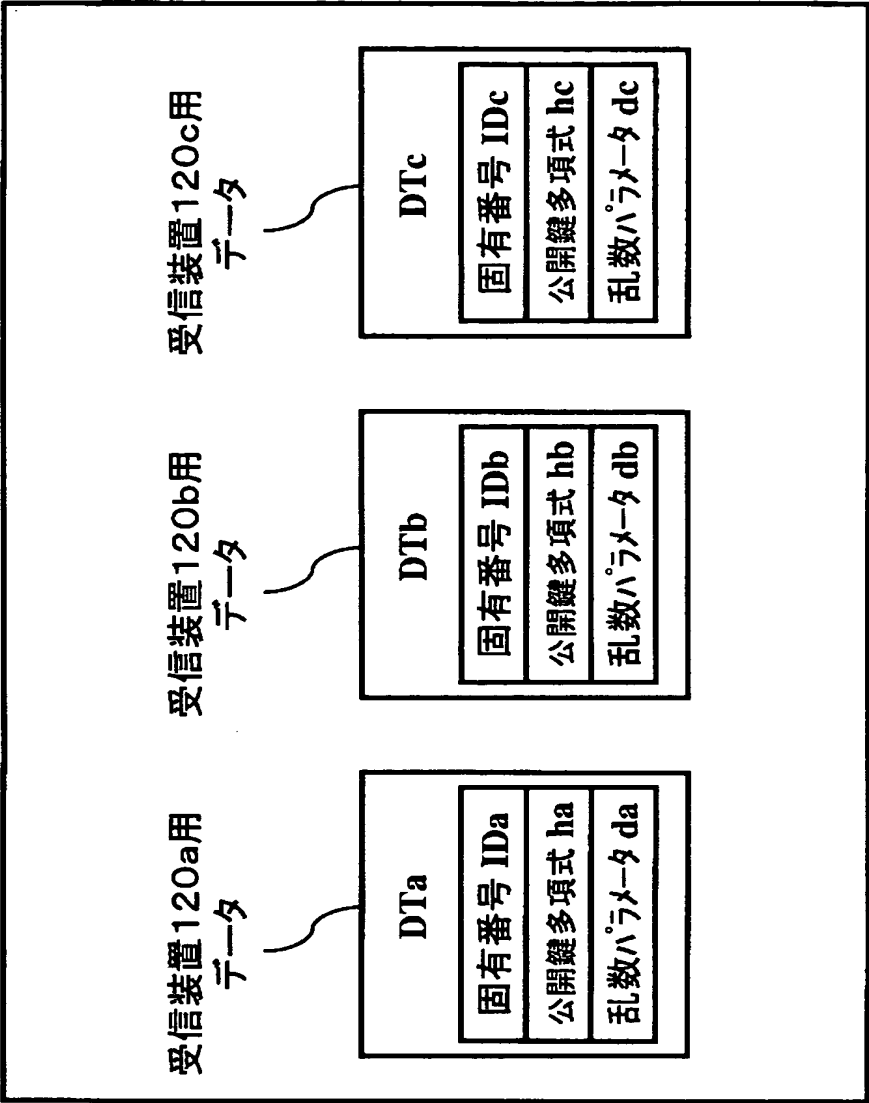


【図 2】

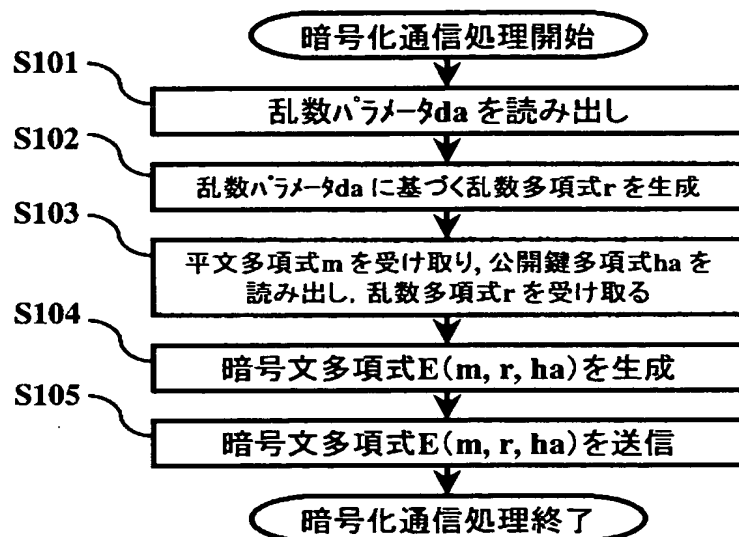


【図 3】

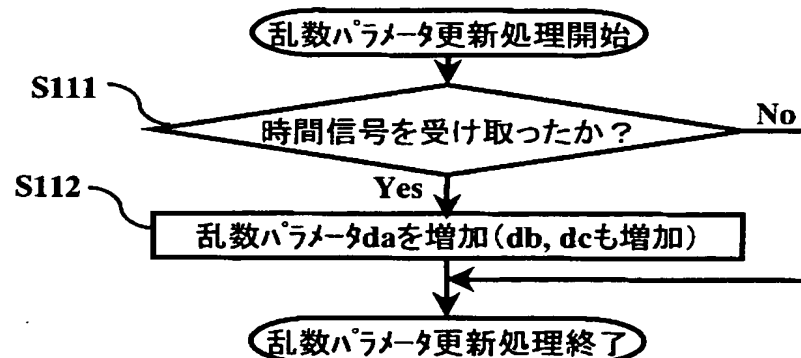
パラメータ記憶部112



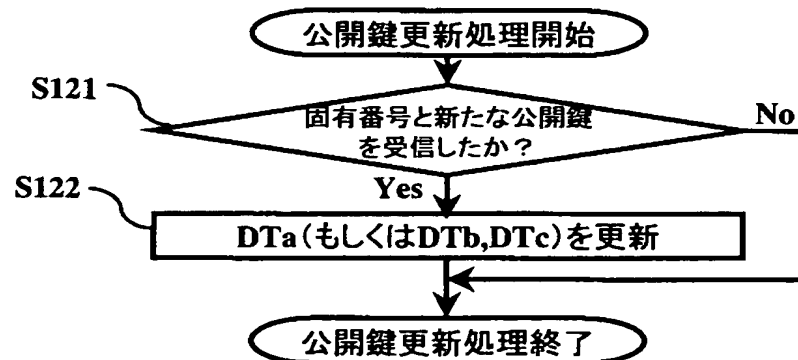
【図 4】



【図 5】

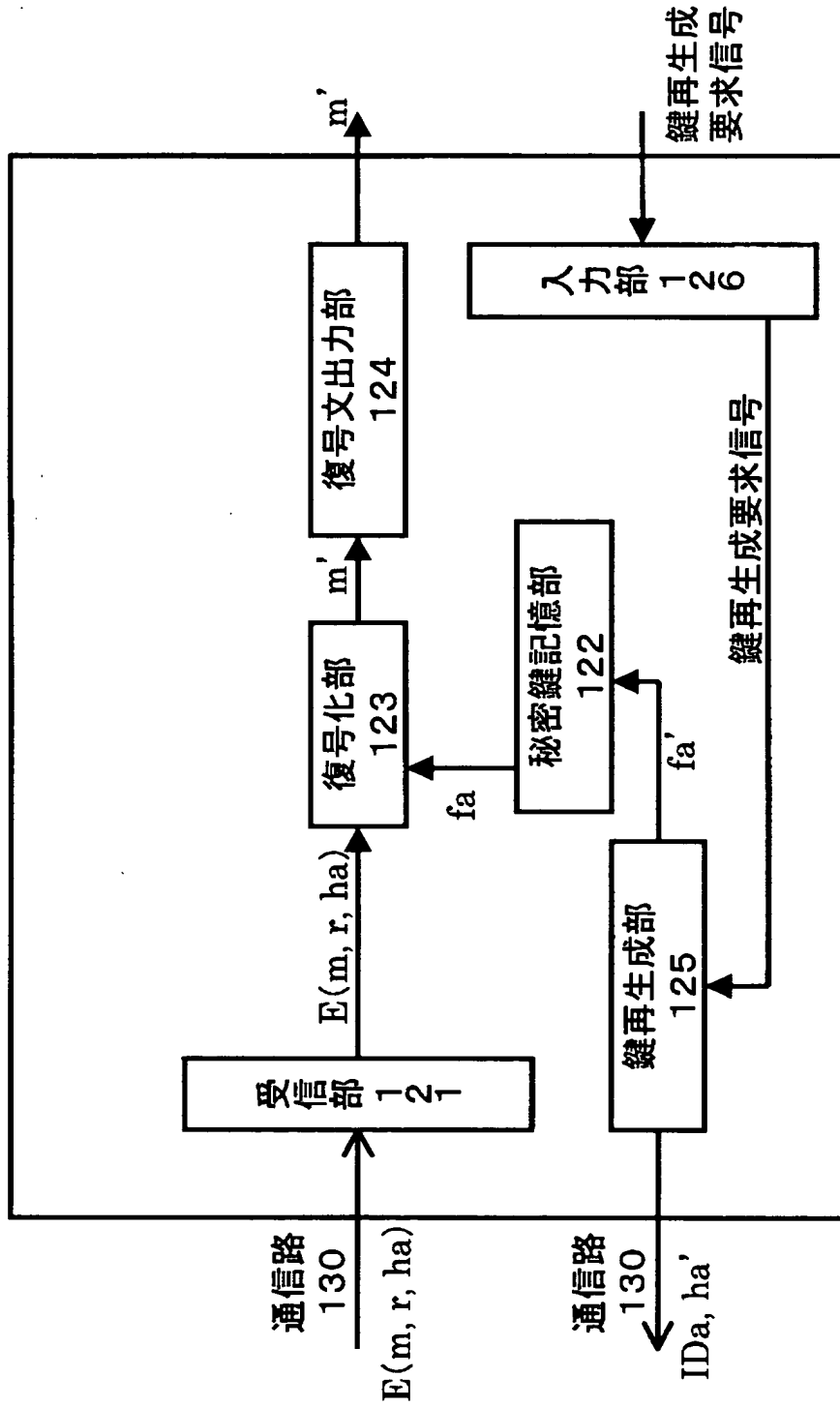


【図 6】

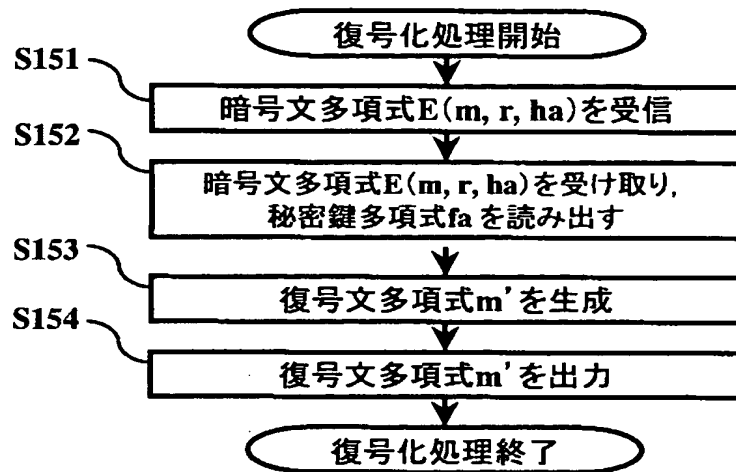


【図 7】

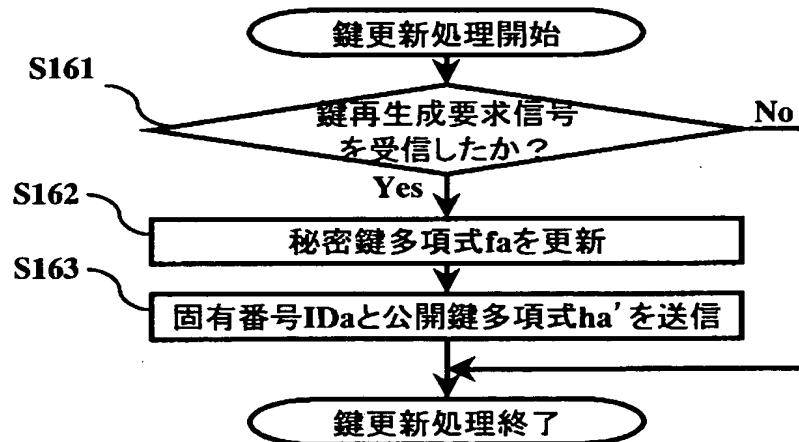
受信装置 120a



【図 8】



【図 9】

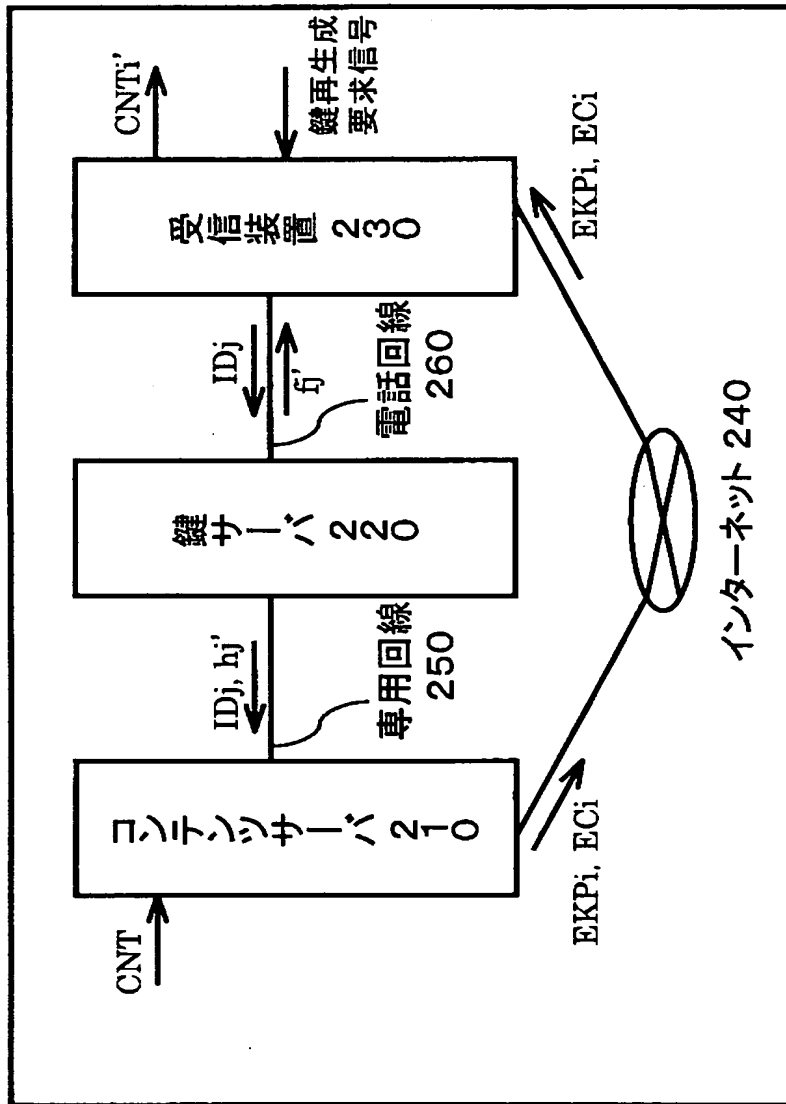


【図 1 0】

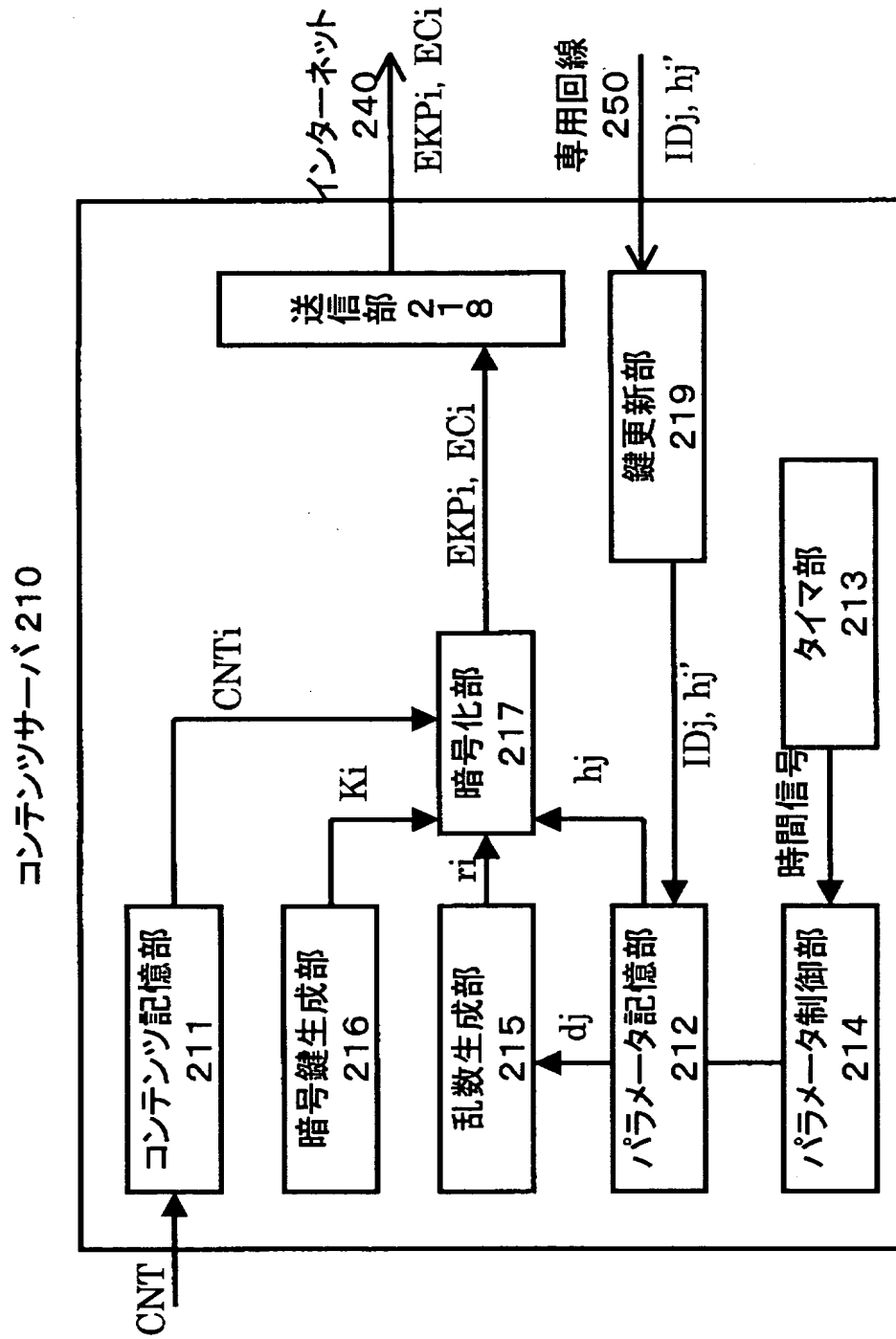
乱数パラメータ d	18	28	38	48	58	68	78
復号エラー発生率(%)	0.0007	0.09	2.6	2.3	7.1	13.7	24.8

【図 11】

暗号システム 2

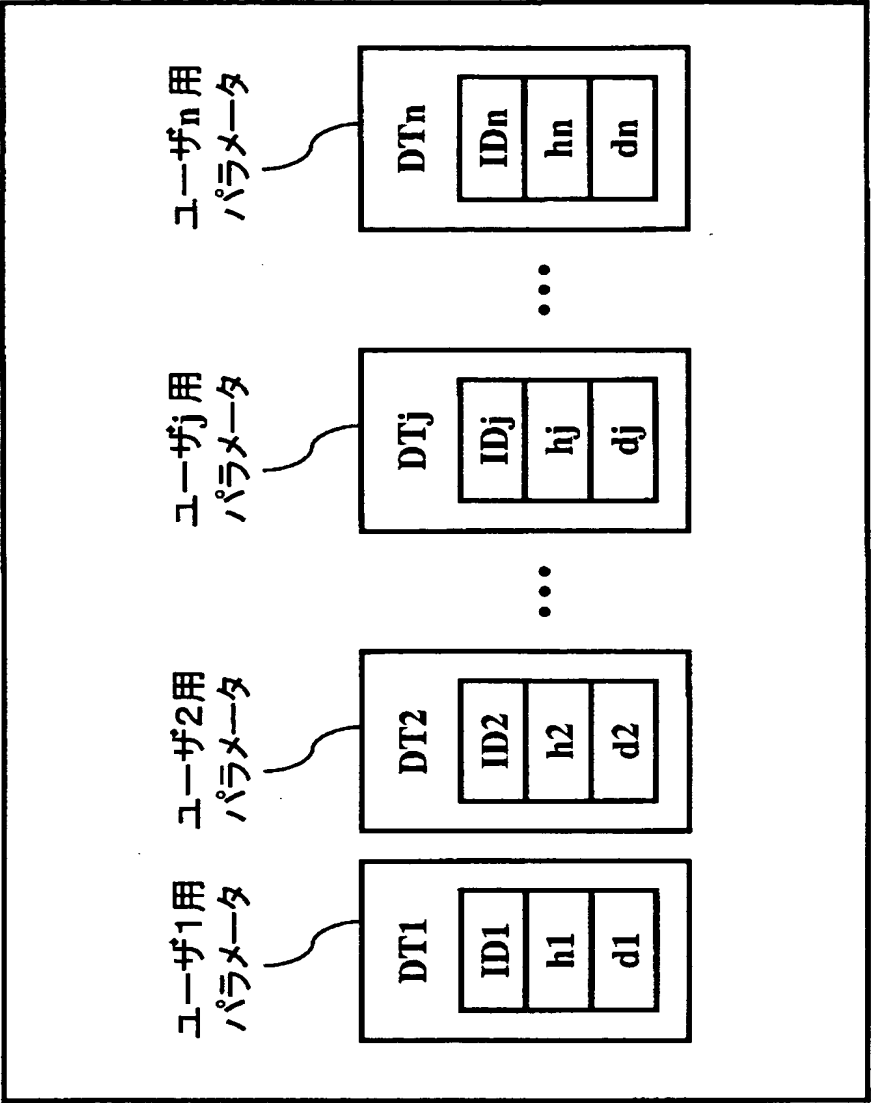


【図 12】

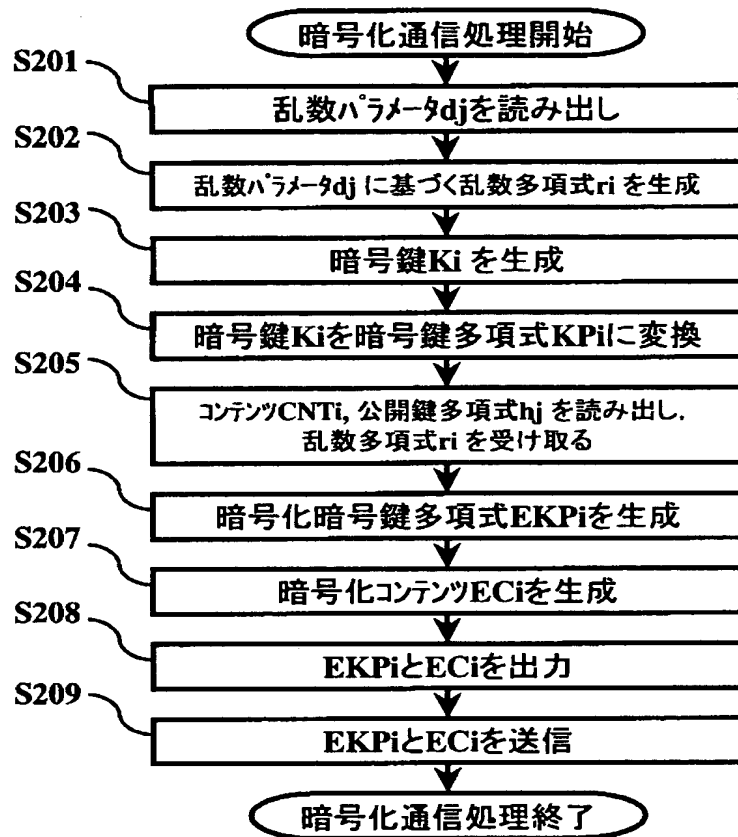


【図 1 3】

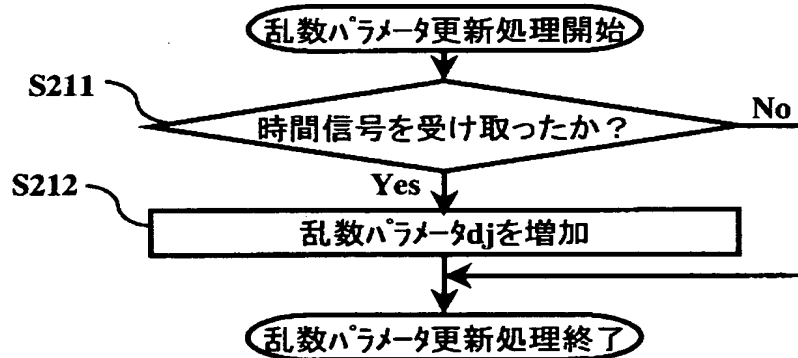
パラメータ記憶部 212



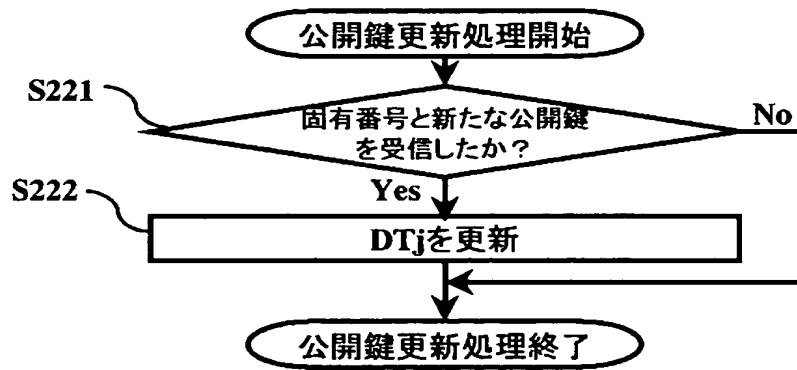
【図 1 4】



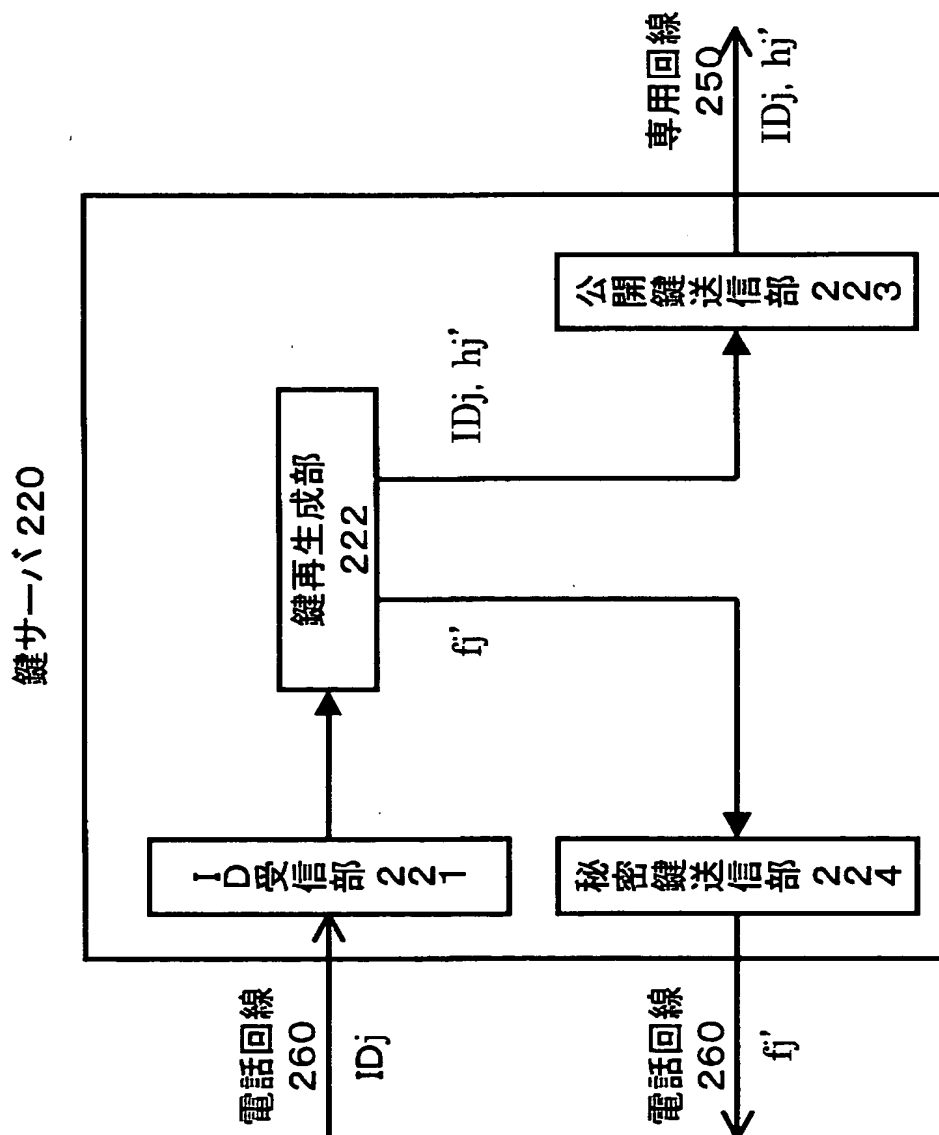
【図 1 5】



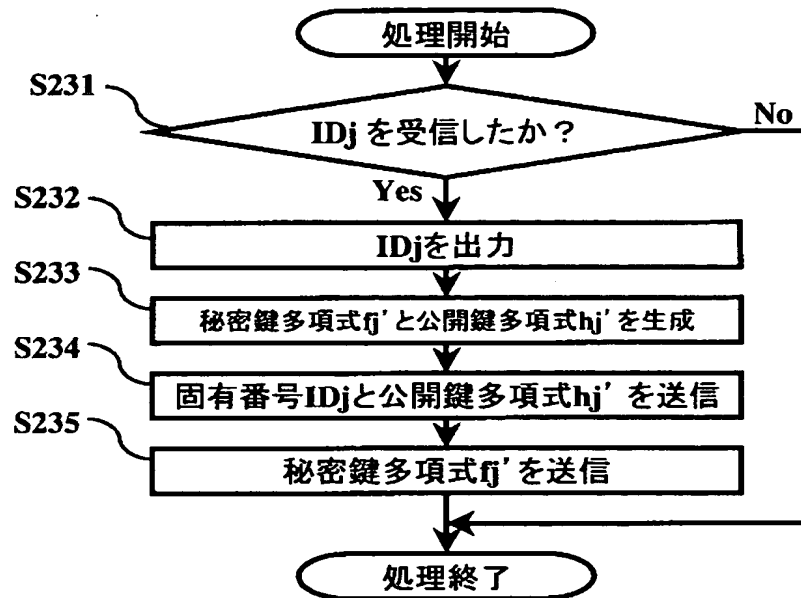
【図 16】



【図 17】

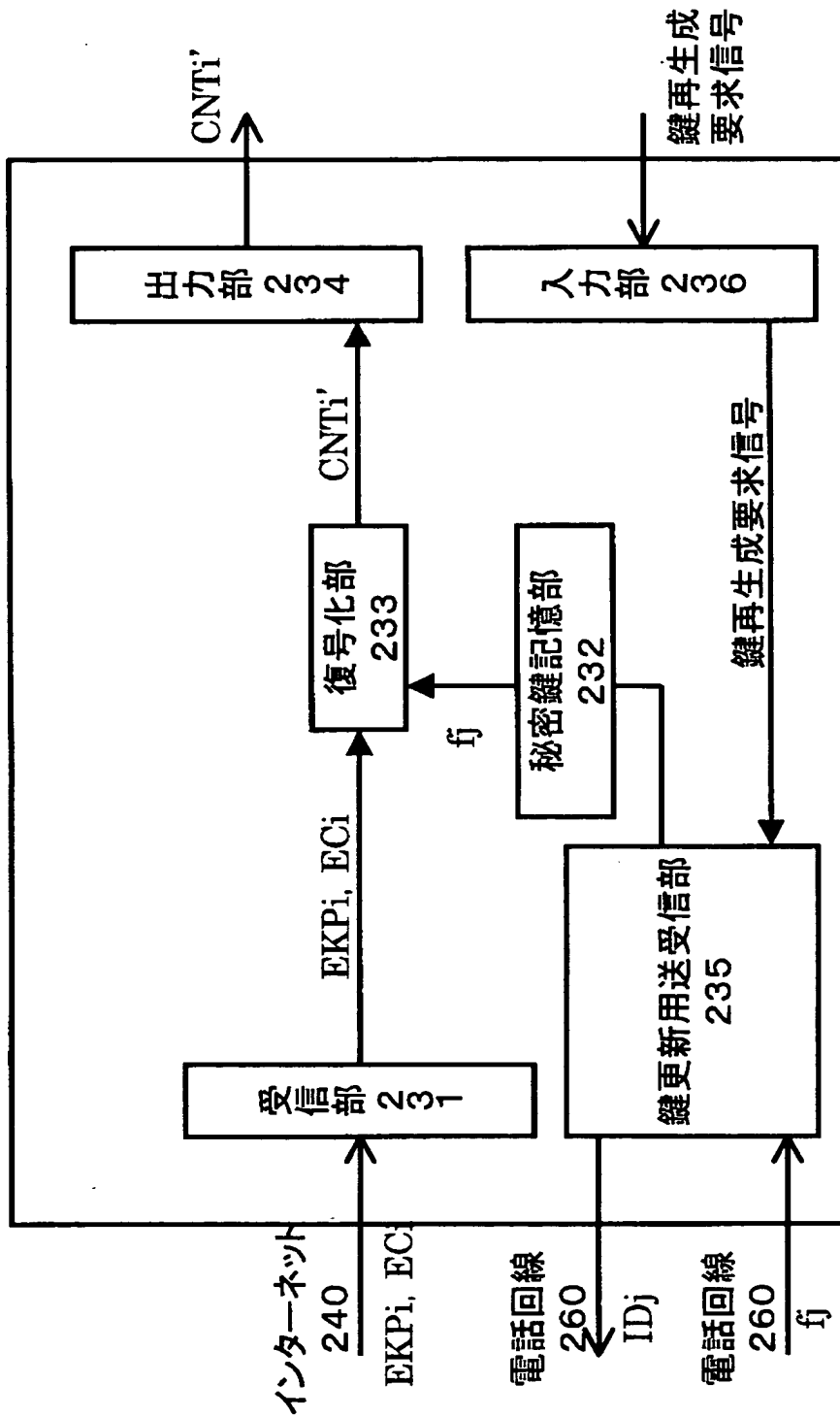


【図 1 8】

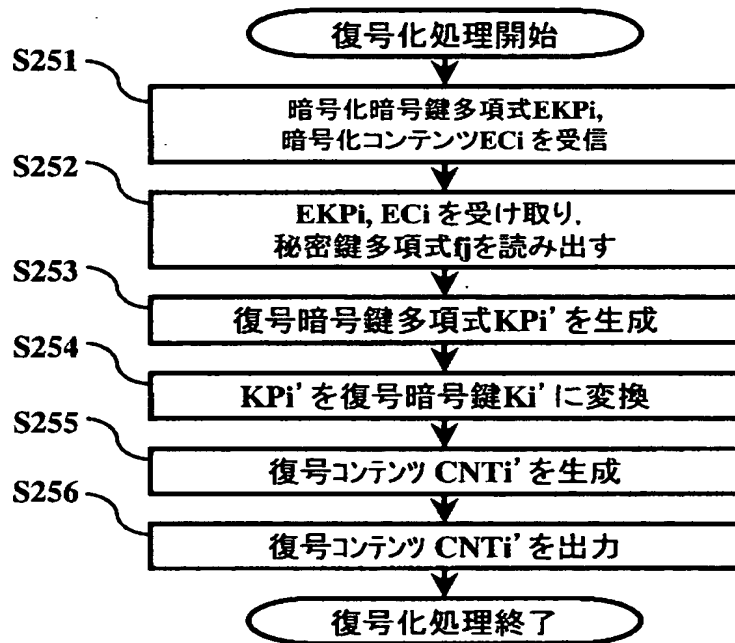


【図19】

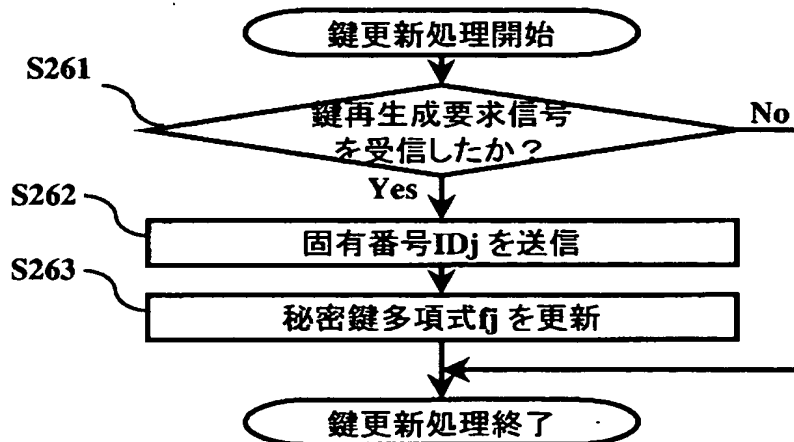
受信装置 230



【図 2 0】



【図 2 1】



【書類名】 要約書

【要約】

【課題】 送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第1の目的とする。

【解決手段】 本発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社